BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-112

7 APRIL 2006

Communications and Information

INFORMATION TECHNOLOGY HARDWARE ASSET MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFCA/SYND
Supersedes AFI 33-112, 25 February 2001

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 72

This Air Force instruction (AFI) implements Air Force Policy Directives (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; 33-2, *Information Protection* (will become *Information Assurance*); and 10-6, *Mission Needs and Operational Requirements*; by identifying responsibilities for supporting Air Force information technology (IT) equipment (computer systems). Some paragraphs in this instruction that do not apply to non-Air Force-managed joint service systems, are marked *(NOT APPLICABLE TO NON-AIR FORCE-MANAGED JOINT SERVICE SYSTEMS)*. This instruction applies to Air National Guard (ANG). Refer technical questions about this instruction to Headquarters Air Force Communications Agency (HQ AFCA/EVPS), 203 West Losey Street, Room 3065, Scott AFB IL 62225-5222. Send recommended changes or comments to HQ AFCA/EASD, 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using Air Force (AF) IMT 847, **Recommendation for Change of Publication**, with an information copy to the Office of the Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Director of Information, Services and Integration (SAF/XCI), 1250 Air Force Pentagon, Washington DC 20330-1250. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records,* (will become AFMAN 33-363) and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds_series.cfm**. See **Attachment 1** for a glossary of references and supporting information. **Attachment 2** contains an address listing of key organizations. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This change incorporates interim change IC 2006-1 (**Attachment 6**). It changes the name to *Information Technology Hardware Asset Management*. The main focus is to expand information technology (IT) asset management focus from computer system management to IT hardware asset management, remove all references to the Information Processing Management System (IPMS) and add references to the Asset Inventory Management (AIM) module of the Air Force Equipment Management System (AFEMS). It

also incorporates numerous office symbol changes to reflect Secretary of the Air Force (SAF/XCI), HQ USAF/ILC, HQ USAF/CIO, HQ USAF/XI, Headquarters Standard System Group (HQ SSG), and AFCA transformation. Paragraph **1.** is changed to reflect SAF/XCI instead of Headquarters United States Air Force (HQ USAF/SC) and further define responsibilities of the Air Force Computer Systems Management Working Group (CSMWG). Paragraph **2.** is changed to define SAF/AAZ's cognizance over networks processing Special Access Program/Special Access Required information. Paragraph **3.** defines AFCA responsibilities. Paragraph **4.** is changed to update the training responsibilities of Headquarters Air Education and Training Command (HQ AETC). Paragraph **5.** is modified to change program management of the Air Force IT asset management system from HQ SSG to the Headquarters Operations and Sustainment Systems Group (HQ OSSG) and removes references to IPMS. Paragraph **6.** changes to the responsibilities of the Communications and Information Systems Officer (CSO). Paragraph **6.12.** is changed to provide detailed criteria for appointing the primary and alternate equipment control officer (ECO). Paragraph **7.** updates the organizational commander's duties. Changes include the requirement for the commander to sign the annual inventory listing and detailed criteria for appointing equipment custodians. Paragraph **7.14.** is deleted. Paragraph **7.15.**was added to ensure compliance with the Department of Defense (DOD) policy for disposition of computer hard drives. Paragraph **8.** is deleted. The organization computer manager responsibilities previously defined in paragraph **8.** are performed by Client Support Administrators (CSA). Guidance for CSAs is found in AFI 33-115, Volume 1, *Network Operations (NETOPS)*. Paragraph **9.** removes references to IPMS and defines the grade requirements and appointing official for the major command equipment control officer (MECO). Paragraph **10.** removes references to IPMS, updates ECO responsibilities, and clarifies inventory procedures. Paragraph **10.** also requires the ECO to update the asset status in AIM upon receipt of IT hardware assets. Paragraph **11.** updates equipment custodian responsibilities. Paragraph **11.1.1.** requires the commander's signature in the AIM inventory listing. Paragraph **11.16.** is added to direct the equipment custodian (EC) to coordinate with the Information Systems Security Officer (ISSO) for hard drive sanitation according to the procedures outlined in Air Force Systems Security Instruction (AFSSI) 5020 (FOUO), *Remanence Security*. Paragraph **12.** is deleted. Paragraph **13.** is deleted. Paragraph **14.** directs users to refer to AFI 33-202, Volume 1, *Network and Computer Security*. Paragraphs **14.1.**, **14.2.**, and **14.3.** are deleted. Paragraph **15.** is expanded to define Air Force contractor responsibilities for funding, accountability and Chief Financial Officer reporting. Paragraph **16.** removes references to IPMS and changed to Acquisition of Information Technology (IT) Assets. Paragraph **16.1.** makes procurement of desktops and laptops through Air Force Way (AFWay) mandatory unless waived by the major command (MAJCOM) Chief Information Officer (CIO)/A6. Paragraphs **17.** and **18.** are deleted. Deployment considerations listed in paragraph **17.** are moved to paragraph **6.** under CSO responsibilities. Paragraph **19.** includes policy for use of all IT assets. Paragraph **19.2.** is added to instruct personnel not to input or store government information/data on privately-owned IT assets without approval of the Designated Approving Authority (DAA) according to AFI 33-202, Volume 1. Paragraphs **19.2.1.**, **19.2.2.**, **19.3.**, and **19.4.** are deleted. Paragraph **20.** is changed to include Personal Digital Assistants (PDA). Paragraph **21.** is changed to include procedures for the exchange or sale of government automated resources programs. Paragraph **22.** is changed to Inventory Management and Accountability of IT Hardware Assets. Paragraph **22.1.** is changed to provide a link on the Air Force Portal to a comprehensive and current list of accountable and non-accountable assets to help determine the accountability of IT assets. Paragraph **22.1.1.** is added to assign management and oversight of the official Air Force accountability list to the CSMWG. Paragraphs **23.**, **24.**, and **25.** are deleted. The requirement in paragraph **24.** to use labels for identification of IT assets is moved to paragraph **6.15.** Paragraph **26.** removes references to IPMS. Paragraph **27.** removes maintenance practices specific to computer systems and applies maintenance concepts for IT assets. Changes to paragraph **27.** also require the CSO to estab-

lish a Logistics Support Plan to ensure logistics support for IT assets throughout the expected lifecycle and offers methods to compute operational spares. Paragraph **28.** is deleted. Paragraph **29.** includes maintenance reporting for IT assets. Paragraphs **30.** and **31.** are deleted. Paragraph **32.** is changed to encompass IT assets instead of computer systems. Paragraph **33.** defines excess and implements procedures to dispose of excess through AIM. Changes also require IT assets picked up as excess to be accounted for in AIM. Cannibalization guidelines for spare parts are now included in paragraph **27.** Paragraph **34.** reflects procedures for obtaining excess IT assets in the AIM environment. Paragraph **35.** changes transferring excess IT assets to the Defense Reutilization Marketing Office (DRMO). References to the Computers for Learning Program and Executive Order (E.O.) 12999, *Education Technology: Ensuring Opportunity for All Children in the Next Century*, are also added to Paragraph **35.** Paragraphs **36.** and **37.** are deleted. Paragraph **38.** adds reference to the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). **Attachment 1** is updated as a glossary of references and supporting information. **Attachment 2** is deleted. **Attachment 3** provides a checklist for IT assets and to comply with this IC. **Attachment 5** is added to show AIM asset status codes. A bar (|) indicates a revision from the previous edition.

Section A—Responsibilities

1. Office of the Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Director of Information, Services and Integration (SAF/XCI):

1.1. Develops, publishes, and disseminates Air Force doctrine and policy for information technology (IT) asset systems.

1.2. Identifies formal IT management training requirements.

1.3. Resolves management issues on IT hardware assets accounted for in the Asset Inventory Management (AIM) module and resolves policy disagreements between major commands (MAJCOM), functional managers, and non-Air Force agencies.

1.4. Acts as functional manager for the IT component of the Air Force Equipment Management System (AFEMS). The IT hardware component of the AFEMS is called the AIM module.

1.5. DELETED.

1.6. Sets policy and works in conjunction with Defense Logistics Agency (DLA/DRMS) on disposition of excess IT assets.

1.7. DELETED.

1.8. DELETED.

1.9. DELETED.

1.10. DELETED.

1.11. Establishes and chairs the Air Force Computer Systems Management Working Group (CSMWG) that directly supports CSM personnel at all levels including MAJCOM Equipment Control Officers (MECO), Communications and Information Systems Officers (CSO), Equipment Control Officers (ECO), organizational commanders and computer equipment custodians (EC) in the execution of their responsibilities as delineated in this instruction. The CSMWG provides broad representation allowing for improved cross feed of information and feedback from the field necessary to make informed decisions about CSM policy and procedures. The CSMWG serves as the Air Force CSM management infrastructure to deal with all CSM-related issues in an efficient and effective manner.

1.11.1. DELETED.

1.11.2. The CSMWG will:

1.11.2.1. Develops proposed solutions on issues affecting IT system life-cycle management.

1.11.2.2. Identifies functional improvement opportunities for review, prioritizing, approval, and budgeting considerations.

1.11.2.3. Advises Air Force leadership on IT management issues.

1.11.2.4. Defines new functional requirements and provides oversight to automated information systems (AIS) processes supporting Air Force IT management.

1.11.2.5. Works with the IT Commodity Council on procurement initiatives.

1.12. Issues communications-electronics (C-E) maintenance management policy (see AFI 21-116, *Communications-Electronics Maintenance Management*). The intent of AFI 21-116 is to ensure only

qualified personnel perform maintenance to avoid unnecessary risks to personnel and prevent damage to C-E equipment.

2. Administrative Assistant to the Secretary of the Air Force, Security and Special Programs Oversight (SAF/AAZ).

2.1. Provides policy and oversight on computer security pertaining to networks processing Special Access Program/Special Access Required information in their role as Special Access Program Coordination Office.

2.1.1. Air Force information technology assets, under the cognizance of the Special Access Program Coordination Office, may be tracked in the AIM module of AFEMS, if the cognizant security authority determines that there are no security concerns. SAF/AAZ provides guidance for meeting regulatory compliance for IT assets that are not tracked in AIM.

3. Headquarters Air Force Communications Agency (HQ AFCA).

3.1. Provides guidance and support to MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) in developing, implementing, and managing IT assets.

3.2. Reviews, evaluates, and interprets issues/problems and makes recommendations to SAF/XCII on policy changes.

3.3. Reviews, interprets, and disseminates Air Force policy.

3.4. Acts as office of primary responsibilities (OPR) for this instruction.

4. Headquarters Air Education and Training Command (HQ AETC).

4.1. Provides formal IT training when directed by SAF/XCI.

5. Headquarters Operations and Sustainment Systems Group (HQ OSSG/LRE).

5.1. Functions as Program Manager (PM) for the AIM module.

5.2. DELETED.

5.3. Submits the special year-end chief financial officer report to the Defense Finance and Accounting Service (DFAS).

5.4. Proposes technical solutions for defined requirements.

5.5. Coordinates all requirements and associated cost data through the program agreement (PA) manager for review and approval.

5.6. Notifies the PA manager of all unfunded requirements.

5.7. Coordinates software releases through the PA manager prior to scheduled release.

5.8. Provides input to program management reviews.

5.9. Completes required Information Support Plan/certification documentation prior to scheduled release.

5.10. Develops and maintains the AIM Computer Based Training (CBT) courseware and AIM User's Manual.

5.11. Provides operations, programming, and software support.

6. Communications and Information Systems Officer (CSO) :

6.1. DELETED.

6.2. Processes all base-user computer systems orders except those excluded by host tenant support agreements and joint service programs managed outside the Air Force.

6.2.1. Ensure users and mission planners use strategy-to-task methodologies and the Air Force modernization planning processes to link IT investments to mission essential task improvements (see AFI 10-1401, *Modernization Planning Documentation*). The CSO integrates these requirements into the base Communications and Information Systems blueprint.

6.3. Is the accountable officer for all IT hardware equipment listed in their assigned AIM account. Ensures the AIM inventory is used to provide accountability of all base IT hardware resources assigned to that Defense Reporting Activity (DRA). Refer to paragraph **22.1.** to determine if a particular piece of IT hardware equipment should be accounted for using methods or systems other than AIM.

6.3.1. DELETED.

6.3.2. DELETED.

6.4. Assists in planning and execution of all activities related to the deployment of systems.

6.5. Assists the supporting contracting officers in developing an acquisition strategy for maintenance contracts.

6.5.1. Follows budgeting arrangements established in host tenant support agreements.

6.5.2. DELETED.

6.6. Ensures identification and submission of maintenance requirements, performance work statements and surveillance plans (see AFI 63-124, *Performance-Based Service Contracts [PBSC]*).

6.6.1. Assists the supporting contracting officer in developing an acquisition strategy for maintenance contracts.

6.6.2. Ensures annual review of maintenance strategies and reports to verify organizations use the most cost-effective options.

6.6.3. Advises base organizations of local maintenance procedures.

6.7. DELETED.

6.8. Analyzes IT asset maintenance cost data to assist in developing cost-effective maintenance solutions.

6.8.1. Directs retention of serviceable excess IT assets, when allowed by the parent MAJCOM, for maintenance redundancy or operational spares, by ensuring use of sharing and redistribution programs to meet user requirements.

6.8.2. Authorizes removal/transfer of unserviceable IT assets for spare parts.

6.8.3. Authorizes cannibalization of IT assets to satisfy critical mission requirements. Maintenance actions to obtain assemblies, subassemblies, or parts from spare IT assets are considered transfers and will not be treated as cannibalization actions.

6.9. Authorizes cannibalization of unserviceable computer systems for spare parts.

6.10. Coordinates action to ensure secure, climate controlled, and easily accessible facilities with sufficient floor space are provided to the equipment control officer (ECO) for receiving, storing, and distributing IT assets.

6.11. Coordinates on IT asset requirements with the appropriate office or unit.

6.12. Appoints primary and alternate ECOs and provides a copy of the appointment letter to the MECO. Although no grade restrictions apply for these positions, the primary and alternate ECOs should have the leadership skills and IT asset knowledge necessary to provide guidance and direction to the EC. The recommended minimum rank/grade requirement for the primary ECO is Technical Sergeant/GS-7. An airman (Senior Airman or below) may be appointed as an alternate ECO, if the CSO believes the airman is mature enough to handle the responsibility See paragraph **15.** for contractors. ***NOTE:*** The primary ECO will supervise the alternate ECO in performance of duties and responsibilities.

6.12.1. DELETED.

6.13. DELETED.

6.14. DELETED.

6.15. Where practical (e.g., due to size limitations) ensure mandatory AIM-generated standard product (bar code) labels are used to identify all IT assets within their DRA.

7. Organization Commanders or Equivalent. Commanders or their equivalent with IT assets are responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to IT assets under their control. The accountable officer is responsible for all IT assets within their organization.

7.1. Budgets for maintenance of computer systems that are not the responsibility of the CSO.

7.2. Reviews and coordinates on organization's requirement documents.

7.3. Submits unit computer systems requirements to the applicable CSO for technical solutions according to AFI 33-103, *Requirements Development and Processing*.

7.4. Reviews assigned IT assets annually to determine if the IT is obsolete, still meets user requirements or needs modification and act accordingly.

7.5. Appoints, in writing, primary and alternate ECs, no later than 45 days prior to the projected departure of the current EC. According to AFMAN 23-110, Volume 2, Part 2, Chapter 22, ECs may be military (see note) or civilians. Contractors may also be ECs according to AFI 23-111, *Management of Government Property in Possession of the Air Force,* if the contract so stipulates and must be mutually agreeable to the organization commander and the CSO. This applies to active duty, guard, and reserve personnel. Foreign nationals or local wage rate employees (foreign nationals in host countries) may be appointed primary or alternate custodians only when they may be held pecuniary liable under the law of the host country. Organization commanders must review the provisions and restric-

tions outlined in AFI 31-501, *Economic Analysis*, AFI 33-202, Volume 1, *Network and Computer Security*, and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, before appointing foreign nationals as primary or alternate equipment custodians. ***NOTE***: An airman (Senior Airman or below) may be appointed primary or alternate custodian by the organization commander, if the commander believes the airman is mature enough to handle the responsibility.

7.5.1. Sends the EC appointment letter and request for EC training to the ECO.

7.5.1.1. The EC appointment letter should be dated and contain the names of the primary and alternate ECs. The appointment letter should also contain the date the primary and alternate EC received training from the ECO.

7.5.1.2. Ensures the primary or alternate EC is scheduled for training with the ECO within 30 days of initial appointment and annually thereafter.

7.5.1.3. Annually reviews EC appointment letters and training dates to ensure the primary and alternate EC names are current and they have completed annual EC training. After the review, send a new EC appointment letter as described in paragraph **7.5.1.1.** to the ECO. When possible, the review should be held in conjunction with the annual inventory.

7.5.2. Requires departing EC to process out through the ECO.

7.5.3. Ensures outgoing and incoming primary EC conduct and sign a loss-gain joint physical inventory and reconcile missing items under the guidance of the ECO, not later than 30 days prior to the primary EC being relieved of duty. In deployed locations, the forward commander will determine timeline for transfer of duties based on rotation schedules.

7.5.3.1. Refer to AFMAN 23-220, *Reports of Survey for Air Force Property*, to determine if a Report of Survey (ROS) is required when there are inventory discrepancies that cannot be resolved prior to the custodian departing.

7.6. Ensures the EC performs a complete and accurate annual inventory. After the annual inventory is complete, the Commander signs the inventory listing. The Commander's signature certifies to the ECO that the annual physical inventory is complete.

7.7. Ensures the EC notifies the applicable ECO of any computer systems that are scheduled for deployment.

7.8. Promotes user awareness concerning unauthorized or illegal use of computer systems hardware and software.

7.9. Develops and implements a documented process according to AFI 33-114, *Software Management*, to ensure that all software is free of viruses.

7.10. Ensures all accountable IT assets are reported to the ECO for inclusion in the AIM inventory.

7.11. Ensures that the applicable ECO coordinates on the "Ship To" addressee on all purchase requests or transfers that involve computer systems.

7.12. DELETED.

7.13. DELETED.

7.14. DELETED.

7.15. Ensures compliance with the disposition of Department of Defense (DOD) computer hard drive policy cited in the Office of the Assistant Secretary of Defense (ASD) Memorandum, "Disposition of Unclassified DOD Computer Hard Drives," dated June 4, 2001, or hard drive sanitation in accordance with the procedures outlined in Air Force Systems Security Instruction (AFSSI) 5020 (FOUO). Find additional guidance at **http://iase.disa.mil/policy.html**.

8. DELETED.

9. Major Command Equipment Control Officers .

9.1. The MAJCOM CSO or FOA/DRU equivalent appoints the MECO. Although no grade restrictions apply for this position, the MECO should have the depth and experience necessary to provide guidance and direction to the ECO. Recommend minimum grade be a senior non-commissioned officer (NCO)/GS-9 for this position. When the MECO changes, the MAJCOM CSO notifies SAF/XCII (**safcxiiworkflow@pentagon.af.mil**) and HQ AFCA/EVPS (**afca.evps@scott.af.mil**) by electronic mail (E-mail), so their official listings can be updated with the new name, office symbol, phone number, and E-mail address. The MECO will:

9.1.1. Provide guidance and procedural policy to the ECOs on management of IT hardware assets.

9.1.2. Work with other MECOs to determine reporting procedures of tenant units and continue to work together to resolve any problems that might arise.

9.1.3. Approve or reject transfer of IT assets between losing and gaining commands.

9.1.4. Send applicable ECO concerns about the inclusion and/or exclusion of IT hardware assets in AIM to SAF/XCI, 1401 Wilson Blvd, Ste 600, Arlington VA 22209-2315.

9.1.5. Review finalized excess reports completed by applicable ECOs and ensure appropriate action is accomplished.

9.1.6. DELETED.

9.1.7. Allow ECOs to create and maintain holding accounts for known near-term requirements.

9.1.8. DELETED.

9.1.9. Coordinate on the establishment of a new DRA and the IT data system connectivity, as required.

9.1.9.1. Maintain a copy of the base ECO's appointment letter and AIM Access Request form. The MECO also sends the AIM Access Request to the program management office (PMO).

9.1.9.2. DELETED.

9.1.10. Provide assistance to applicable ECOs in closing out a DRA (e.g., base closures).

9.1.11. DELETED.

9.1.12. Disseminate information provided by HQ USAF, HQ AFCA, and PMO to applicable ECOs.

9.1.13. Establish accountability for IT assets acquired through joint services PMs, as required.

9.1.14. Notify the PMO of centrally managed programs of any excess equipment acquired for that program that is available for reutilization.

10. Equipment Control Officer (ECO).

10.1. The CSO appoints the primary and alternate ECOs according to paragraph **6.12.** See paragraph **15.** for contractors. Due in part to guidelines in AFPD 65-2, *Management Control Program*, the ECO cannot be the EC for the holding account. The unit commander must appoint a different individual as the EC to maintain a separation of duties.

10.1.1. In deployed locations, the forward commander appoints the most qualified individual available to perform the duties of ECO.

10.2. Determine the method used to account for IT according to paragraph **22.1.**

10.2.1. If the IT hardware should be accounted for in AIM, complete all necessary documentation and ensure the IT asset status in AIM is updated using the codes identified in **Attachment 5**. Review the IT asset status codes periodically to ensure the codes reflect the current status.

10.2.2. DELETED.

10.2.3. Assist the EC in determining the ownership of all FOB IT assets.

10.2.4. DELETED.

10.2.5. Direct ECs to conduct a complete annual inventory of all IT assets assigned to the EC's AIM account and an annual review of EC appointment letters to ensure the primary and alternate EC names are current and they have completed annual EC training. When possible, the EC appointment letter review should be held in conjunction with the annual inventory.

10.2.5.1. During the inventory, ensure all assets can be traced back to an AIM inventory listing. If IT hardware equipment is found in the work area that is not on the AIM inventory listing, refer to paragraph **22.1.** to determine if the IT equipment should be added to AIM to establish accountability.

10.2.5.2. In deployed locations, the forward commander determines the timeline for inventory based on rotation schedules.

10.2.5.3. ECOs have the authority to lock EC accounts until the annual inventory and EC training is completed.

10.2.6. DELETED.

10.2.7. Authorize the EC to retain serviceable excess IT asset items for maintenance redundancy or operational spares when allowed by the parent MAJCOM.

10.2.8. Retains unserviceable excess IT asset hardware for cannibalization as directed by the CSO.

10.2.9. Ensure correct MAJCOM code is entered into AIM for all IT assets in their DRA.

10.2.10. Provide the EC with AIM-generated standard product (bar code) labels.

10.2.11. Work with the EC to update the inventory as dictated by a ROS. Use a copy of the DD Form 200, **Financial Liability Investigation of Property Loss**, to adjust accountable records.

10.2.12. Complete out-processing for departing EC upon transfer of account and receipt of new appointment letters and signed joint loss-gain inventory.

10.2.13. Provide guidance and annual training for the EC. Upon request, the ECO provides their commanders with documentation verifying names of the ECs trained, material covered, and training dates.

10.2.14. Take guidance and direction from the MECO and CSO.

10.2.15. DELETED.

10.2.16. Code deployable IT assets in the AIM database.

10.2.17. Establishes accountability for IT hardware assets acquired through joint services, working with the parent MAJCOM.

10.2.18. Attempt to reutilize excess organizational IT assets that meet minimum architecture standards before offering equipment to organizations outside the DRA, when allowed by the parent MAJCOM.

10.2.19. DELETED.

10.2.20. DELETED.

10.2.21. After receipt of a transportation fund cite, direct the losing custodian to prepare the necessary shipping documents for items that are excess and required by other services.

10.2.22. DELETED.

10.2.22.1. DELETED.

10.2.23. DELETED.

10.2.24. DELETED.

10.2.25. Works with any tenant ECO to establish a host tenant agreement identifying any assistance required, such as AIM connectivity.

10.2.26. DELETED.

10.2.27. DELETED.

10.2.28. Coordinate on all host-tenant support agreements (HTSA) concerning IT asset management. IT accountability support can be specified in the HTSA or a Memorandum of Agreement (MOA).

10.2.29. DELETED.

11. Equipment Custodians (EC).

11.1. Accountable for all assigned IT hardware assets in their account and will:

11.1.1. Perform, at a minimum, an annual physical inventory of all items in the account. Also, conduct inventories when directed by the ECO. Upon completion of the inventory, the EC and the organizational commander or equivalent sign the inventory with the original copy retained by the EC and a copy for the ECO file.

11.1.2. Only the most current inventory is retained in the EC/ECO folder. Review past inventory records before disposing of old inventory data and ensure source documents are retained to sup-

port current inventory records, e.g., Reports of Survey, hand receipts, etc. Recommend using 6-part folders.

11.2. When practical (e.g., due to size limitations), ensure all accountable IT assets have AIM-generated standard product (bar code) labels affixed.

11.3. Obtain approval and coordinate all potential transfers of IT assets between EC accounts with the applicable ECO where practical.

11.4. Report all FOB IT assets to the applicable ECO and accept accountability or distribute equipment as directed by that ECO.

11.5. Sign for new equipment received through the ECO.

11.6. Take guidance from the ECO on all shipments, transfers, donations, or turns-ins of excess IT assets.

11.7. Provide appropriate documentation to the applicable ECO to clear the account of equipment that was shipped to another base/location, transferred to another account, donated to a school, or turned-in to the DRMO.

11.8. Remain responsive to applicable ECO.

11.9. Must out-process through the applicable ECO.

11.10. Conduct a joint physical inventory (outgoing EC with incoming EC) and reconcile any missing items, via ROS or hand receipt, before permanent change of station, permanent change of assignment, separation, or retirement (minimum of 30 days prior). Contact the individual to whom the equipment was issued, to verify the equipment's status.

11.11. DELETED.

11.12. Initiate the ROS process according to AFMAN 23-220, concerning any lost, damaged, or destroyed IT assets.

11.13. Notify the applicable ECO of excess IT assets.

11.14. Provide the applicable ECO a serialized numbered list of any deployed IT assets.

11.15. Receive and secure all IT assets, if not received by the ECO, until proper accountability is established.

11.16. Coordinate with the Information Systems Security Officer (ISSO) to ensure the ISSO sanitizes hard drives according to the procedures outlined in AFSSI 5020 (FOUO). Find additional information at **http://iase.disa.mil/policy.html**

12. DELETED.

Section B—General Guidance and Procedures

13. DELETED.

14. Network and Computer Security. Refer to AFI 33-202, Volume 1.

14.1. DELETED.

14.2. DELETED.

14.3. DELETED.

15. Air Force Contractors. Organizational commanders grant contractors access to, or allow operation of, government-furnished or contractor-owned IT resources processing government information.

15.1. Contractors may function as equipment custodians (if so stipulated in the contract) for DOD-owned IT assets as the contract specifies.

15.2. According to the Federal Acquisition Regulation (FAR) 45.505, *Records and Reports of Government Property*, the contractor's property control records shall constitute the Government's official property records unless an exception has been authorized. The contractor shall establish and maintain adequate control records for all Government property, including property provided to and in the possession or control of a subcontractor.

15.3. Annually, the contractor's property control system shall provide to the contracting official, the total acquisition cost of Government property for which the contractor is accountable under each contract with each agency, including Government property at subcontractor plants and alternate locations. (Reference FAR Part 45.)

15.4. Establish the extent of contractor liability in the provisions of the applicable contract's government property clause. (See AFI 23-111.)

15.5. If a contractor is hired to accomplish ECO duties, the Air Force retains responsibility for obligating funds and receiving assets as they are inherently governmental functions. (See FAR 7.5, *Inherently Governmental Functions*)

15.6. The functions and responsibilities of the Accountable Officer are defined by DOD 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, January 2002. Accountable Officers exercise substantive discretionary authority in determining the Government's requirements and controlling Government assets. The responsibilities of the Accountable Officer and the position of the Accountable Officer are not contractible.

15.7. Contractors can perform functions in support of the Accountable Officer and functions where they are performing in accordance with criteria defined by the Government. For instance, contractors can process requisitions, maintain stock control records, perform storage and warehousing, and make local procurements of items specified as deliverables in the contract.

15.8. The responsibility for administrative fund control is inherently governmental. The contractor can process all required paperwork up to funds obligation, which must be done by the Government employee designated as responsible for funds control. The contractor can also process such documents as reports for survey and adjustments to stockage levels, but approval must rest with the Accountable Officer. In all cases, the administrative control of funds must be retained by the Government, since contractors or their employees cannot be held responsible for violations of the United States Code.

15.9. If the contractor's property control system does not automatically accomplish Chief Financial Officer asset reporting, then reporting will be accomplished manually according to Federal Financial Accounting Standards No. 6, dated 1996.

16. Acquisition of Information Technology (IT) Assets.

16.1. Procurement of desktops and laptops through AFWay is mandatory unless waived by the MAJCOM CIO/A6. Ordering information can be found at: **https://afway.af.mil**.

16.2. Requirements processing for IT assets not procured through AFWay are covered under AFI 33-103. Process all base user computer systems orders except those excluded by host tenant support agreements and Joint Service programs managed outside the Air Force through AFWay.

16.3. IPMS Ordering Module:

16.3.1. All centralized PMOs that order computer systems or equipment from a standard Air Force infrastructure contract for multiple MAJCOMs must enter and maintain vendor contract, cost, and group tables in IPMS as specified by HQ SSG/ENEI. Make sure these tables, and all subsequent updates, are available in IPMS before the effective date of the initial release or update. Additionally, process all orders for computer systems or equipment from a standard Air Force infrastructure contract through an ordering module in IPMS. Provide funding support for maintaining these tables and the ordering module to HQ SSG/ENEI by the contract PMO. Provide HQ SSG/ENEI sufficient lead time for implementation of the ordering module before the effective date of the contract or update. This ordering module must provide the functionality specified by HQ SSG/ENEI. This functionality, with the other IPMS modules, must, at a minimum, provide:

16.3.1.1. Automatic creation, addition, and, or modification of inventory records to the gaining organization's IPMS database when specific contract orders are processed.

16.3.1.2. Validation of inventory record data field in the IPMS database.

16.3.1.3. Standardized inventory record data entry.

16.3.1.4. Reliable inventory tracking and life-cycle management of computer systems and equipment processed through IPMS.

16.3.1.5. Oversight of funding and computer system/equipment redistribution requirements.

16.4. (DOES NOT APPLY TO ANG) All MAJCOM centralized PMOs ordering computer systems from their own unique contracts (with a total annual funding of $2 million or more in any one year, or $25 million or more over the program life cycle) must comply with the vendor contract, cost, and group table requirements, plus the ordering module requirements, outlined in paragraph **16.3.1.**

16.4.1. MAJCOMs managing the contract must provide funding to HQ SSG/ENEI. PMOs can access IPMS for this input by going through either their MECO or MAJCOM IPMS coordinator. Use MAJCOM-unique contract tables for MAJCOM non-standard contracts just as you use standard contract tables for Air Force standard contracts.

17. DELETED.

18. DELETED.

19. Use of Information Technology (IT) Systems.

19.1. Use IT assets for official or authorized purposes only. Commanders may authorize use of government resources for personal projects if they determine the use is in the best interest of the Air Force. Document the authorization in an organizational policy letter or by a letter to the individual concerned.

19.2. Do not input or store government information/data on privately owned IT assets without approval by the DAA according to AFI 33-202, Volume 1.

19.2.1. DELETED.

19.2.2. DELETED.

19.3. DELETED.

19.4. DELETED.

19.5. Alternate Work Locations. Unit commanders, in coordination with the local personnel office, may authorize personnel to work at an alternate work location (including the employee's home). Unit commanders may also authorize installation of a PC, applicable software, modems, facsimile machines, and data (telephone) lines to support access at the alternate duty location (see Federal Personnel Manual (FPM) System, FPM Letter 368-1, 26 March 1991, "Federal Flexible Workplace Project;" and Public Law (PL) 104-52, *Telephone Installation and Charges*, STAT 468, Section 620 [31 U.S.C. 1348]). Commanders must consider the cost of providing necessary communications and IT assets services before allowing personnel to work from an alternate duty location.

19.5.1. The unit commander authorizing the alternate work location must:

19.5.1.1. Determines the service is necessary for direct support of the agency's mission.

19.5.1.2. Funds for necessary equipment, software, LAN access, and phone lines necessary to support the mission.

19.5.1.3. Makes sure the alternate work location is an economical option to having the individual work in the office.

19.5.1.4. Authorizes payment for installation and monthly recurring charges.

19.5.1.5. Certifies that adequate monitoring capabilities and safeguards against private misuse exist.

19.5.1.6. Coordinate and document all equipment relocations with the EC before relocating assets.

19.5.1.7. DELETED.

19.5.2. The individual authorized an alternate work location is responsible for providing adequate security against equipment and software loss, theft or damage (physical and virus), or misuse. The individual is also responsible for ensuring use of government equipment and government-provided services at the alternate work location are for official use only.

19.5.3. Prepare a letter for the individual to sign acknowledging their understanding of the basic network security policy. It is also recommended that users complete the Information Assurance Awareness CBT for knowledge and understanding of responsibilities regarding Information Assurance and protection.

19.5.3.1. As a minimum, the letter should stipulate that personal IT equipment cannot be used to store, receive, or process classified information and that all chat/instant messenger programs must be disabled on privately owned information systems.

19.5.4. See AFI 33-202, Volume 1, for additional guidelines on telecommuting.

19.5.5. The authorizing unit will keep those letters on file for the duration of the telecommuters' assignment to that unit. After that, file according to the appropriate rule in AFRIMS RDS, Table T33-07 located at **https://afrims.amc.af.mil/rds_series.cfm**.

20. (DOES NOT APPLY TO ANG) General Officers (GO) and Senior Executive Service (SES) Notebook Computers and Personal Digital Assistants (PDA).

20.1. Active Duty GO and SES personnel, including brigadier general selects, are required to maintain E-mail contact with the Chief of Staff of the Air Force. The GO's or SES' current unit of assignment will purchase a GO and SES notebook computer/PDA through the local communications unit and follow the standard requirement process. If desired by the GO or SES, the notebook computer/PDA may accompany the GO or SES from assignment to assignment. If GOs or SES' decide to take their notebook computer/PDA, they will work with the losing and gaining communications unit to ensure proper inventory accountability. The local EC retains accountability for the notebook computer/PDA until transferred to the new location. (See AFI 33-202, Volume 1.)

20.1.1. DELETED.

20.1.2. When a GO or SES retires or leaves Air Force service; he or she must turn in the notebook computer/PDA to the supporting ECO.

20.1.3. DELETED.

21. Environmental Considerations . Use hardware and software within the environmental parameters defined by the vendor (e.g., power, temperature, humidity, etc.).

21.1. Equipment damage outside these parameters may void the warranty or incur an added cost liability according to the contract constraints.

21.2. Commanders may authorize use outside the environmental parameters if mission requirements dictate (e.g., deployed operations).

Section C—Inventory, Accountability, Transfer, and Reporting of Information Technology (IT) Systems

NOTE: Consult AFI 33-115, Volume 1 for additional guidance in determining the types and quantities of equipment needed to support the network.

22. Inventory Management and Accountability of IT Hardware Assets.

22.1. Guidance for determining the accountability of IT assets is governed by multiple and complex congressional, federal, DOD, and Air Force policies. In order to simplify the determination of Air Force accountable IT assets, a comprehensive and current list of accountable and non-accountable assets is posted and maintained on the Air Force Portal (**https://www.my.af.mil**) under the Enterprise IT Initiatives section.

22.1.1. Management and oversight of the official Air Force accountability list is the responsibility of the CSMWG.

22.1.2. DELETED.

22.2. DELETED.

22.3. DELETED.

22.4. IT resources are shipped to the ECO and marked for the appropriate EC.

22.5. Software purchased with original equipment manufacturer IT is considered an integral part of the system. Therefore, the software must be maintained with the system. If the system is transferred, software and system documentation must accompany the system. Transfer all documentation with the system.

22.6. Software license management is explained in AFI 33-114.

22.7. IT assets that are components of weapons systems or other major systems and are already tracked in AFEMS or another property management system will not be tracked in AIM.

22.8. Equipment that is deployed and remains in possession/use of home station personnel who are deployed should be tracked and managed within the home station inventory. Equipment that is transferred to other units or left forward must be properly transferred from the home station (losing unit) account to an appropriate gaining unit to maintain full accountability.

23. DELETED.

24. DELETED.

25. DELETED.

26. Transferring Non-excess Information Technology (IT) Assets to another Department of Defense Component, Federal Agency, State, or Local Government. The transfer of non-excess IT assets occurs when a function, and the IT assets acquired to support that function, is transferred to another DOD component or Federal agency.

26.1. The losing EC provides the losing ECO with a letter of transfer, signed by the losing commander documenting the transfer of the function and equipment.

26.2. Ensure a DD Form 1149, **Requisition and Invoice/Shipping Document**, is signed and dated by a designated official from the shipping activity (Traffic Management Office or commercial carrier) and the EC. For local transfers where no shipping activity is involved, the gaining and losing EC signs the DD Form 1149.

26.3. The ECO for the losing activity should account for the transferred IT. The ECO should also identify excess IT created as a result of the transfer of a function.

26.3.1. The losing ECO and the gaining ECO or other accountable officer will:

26.3.1.1. Review contracts to terminate maintenance for excess equipment.

26.3.1.2. Assist contracting officials in the transfer of responsibilities to the gaining activity.

26.4. The losing ECO will:

26.4.1. Update the asset status field in AIM using the codes in **Attachment 5**.

26.4.2. Provide information for accountable records to the gaining activity if the gaining activity is not using the same database as the losing activity.

26.4.3. Review all contract obligations with the gaining and losing activity. Pay close attention to any contract termination clauses (applies when extra maintenance has been paid for by the losing organization). Use currently established AIM guidance for the removal of items from an account.

26.4.4. Review IT assets release dates. Give adequate notice to the vendor to preclude payment of extra costs.

26.4.5. Coordinate IT assets release dates with other base functions, if necessary.

26.4.6. Coordinate with ISSO for hard drive sanitation according to the procedures outlined in AFSSI 5020 (FOUO). Find additional information at **http://iase.disa.mil/policy.html**.

26.4.7. Provide the IT system database records or custodian report for the EC to attach to the equipment being transferred as appropriate.

26.4.8. Properly inventory, package, warehouse, and secure equipment when storing IT assets before transfer.

26.4.9. Ensure the IT system database inventory records reflect this transfer of equipment accountability to the receiving organization.

26.4.10. Ensure the AFEMS Help Desk is notified to delete or archive the IT records of the equipment being transferred to a Department of Defense Component, Federal Agency, State, or Local Government.

Section D—Information Technology (IT) Systems Maintenance (Not Applicable to Non-Air Force Managed Joint Service Systems)

27. Support Plan. The CSO develops a Logistics Support Plan for IT assets according to AFI 21-116 to ensure logistics support throughout the expected lifecycle. A support plan includes planning and developing a spare and repair parts support plan, determining initial requirements, acquisition planning, distribution, and replenishment of inventory spares.

27.1. Although there is no one size fits all method to determine the quantity of spare equipment or repair parts to keep on hand, consider technical data such as mean time between failure rates, reliability data obtained from the manufacturer, and order and ship time from the source of supply when analyzing supply support. Personnel should also consider mission impact factors such as single point of failure and/or mission critical items. Ultimately it is the commander's or maintenance superintendent's decision based on past experience for low density/commercial off-the-shelf systems that determine the number of on-hand spares to ensure mission accomplishment.

27.1.1. Regardless of the method used to determine the quantity of spare equipment or repair parts to keep on hand, the rationale/methodology used to determine the quantity must be documented in the Logistics Support Plan.

NOTE: Consult AFI 33-115, Volume 1, for additional guidance in determining types and quantities of equipment needed.

27.2. DELETED.

27.2.1. DELETED.

27.2.2. DELETED.

27.2.3. DELETED.

27.3. DELETED.

27.4. DELETED.

27.5. DELETED.

27.5.1. DELETED.

27.5.2. DELETED.

27.5.3. DELETED.

27.6. Maintenance Management. Maintenance management requirements are necessary to avoid risks to personnel, prevent damage to IT hardware equipment, and ensure IT equipment availability to meet mission requirements (Refer to AFI 21-116, AFI 33-115, Volume 1, and AFI 33-series guidance).

27.7. Personnel performing maintenance tasks on IT hardware follow the maintenance management requirements for mission critical and non-mission critical items according to AFI 21-116.

27.8. The headquarters or field-level unit determines if the IT hardware is considered mission critical or non-mission critical for maintenance management purposes.

27.9. Cannibalization may be used to satisfy an existing requirement and to meet priority mission requirements.

27.10. Technical Order 00-20-2, *Maintenance Data Documentation*, outlines the cannibalization process and documentation requirements.

27.11. When cannibalization is the only option available, identify the end item to be cannibalized, and request approval from the chief of maintenance/chief of mission systems flight, computer systems officer or designated representative according to AFI 21-116.

27.12. The CSO or designated representative can approve cannibalization of non-mission critical IT equipment, however; the CSO ensures procedures are developed to ensure non-mission critical cannibalized IT assets are restored to full operational capability if economically feasible.

27.13. Maintenance actions to obtain assemblies, sub-assemblies, or parts are considered transfers and are not treated as cannibalization actions. The CSO may retain assemblies, sub-assemblies, or parts from spare IT assets for maintenance redundancy and operational spares when the communications unit has a maintenance or operational support mission.

27.14. The CSO may also approve the use of unserviceable IT hardware assets as a source for spare parts to maintain other IT equipment. This authority should only be used when allowed by the parent MAJCOM and a cost analysis clearly determines it is economically feasible to use excess assets instead of procuring new items.

27.15. Assemblies, sub-assemblies, and parts obtained for maintenance redundancy or operational spares using the methods described in paragraphs 23.4 and 23.5 are accounted for in the AIM. Ensure the IT asset status in the AIM is updated to identify these items as operational spares. Asset status codes are listed in **Attachment 5**.

28. DELETED.

29. Information Technology (IT) Systems Maintenance Reporting. Users with maintenance contracts document all IT asset maintenance on AF Form 597, or vendor maintenance forms as specified in the appropriate contract. If AF Form 597 is used, provide a copy to the vendor. Each MAJCOM CIO/A6 will specify procedures for logging, documenting, collecting, processing, and filing copies of maintenance records in accordance with the AFI 37-100 series publications (will convert to AFI 33-300 series publications).

30. DELETED.

31. DELETED.

32. Computation of Payments. Contracts applying to managed IT assets.

32.1. Effective Start Date for Rental or Lease. The effective date for rented/leased IT assets is usually the first day of the successful acceptance test. A government-caused acceptance test delay may require payment for the delayed period. Consult the individual contract for specific guidance.

32.2. Computing Charges. ECOs compute charges for rented/leased IT assets, using the reverse side of AF Form 597 or locally produced vendor form.

32.3. Validating Services. For Air Force-managed systems, the verifying activity refers to the equipment utilization reports and the input to the reports (IT assets/equipment orders, AF Form 597, and other appropriate records), to validate the services. Submit claims for credit within 60 days (or as stated in the contract). The IT assets contract manager designates the verifying activity for non-Air Force managed systems (e.g., joint service systems).

Section E—Disposition of Excess Information Technology (IT) Resources

33. Excess. An item is considered excess when it is no longer required due to mission change, equipment upgrades, technology changes, obsolescence, etc. The item is also considered excess when the total quantity on hand exceeds the required quantity, as identified in the technical solution/requirements document, plus the number of authorized spares as identified in the Logistics Support Plan. According to AFI 23-111, accountable individuals are responsible for properly identifying, reporting, and determining correct disposition of unserviceable, reparable, or excess property.

33.1. Base or MAJCOM CSOs may develop their own policies for the retention of excess IT assets, to include potential reutilization (see AFSSI 5020 [FOUO]). However, the rationale for the retention policy must be documented; preferably in the Logistics Support Plan.

33.2. The EC notifies the ECO when IT assets become excess. If possible, ECs should provide notification 30 days before the equipment goes off line to allow completion of the screening cycle while the equipment is still in use, eliminating the need to store excess assets. Until receipt of final disposition instructions, the EC stores the equipment to prevent damage, deterioration, or unauthorized cannibalization.

33.3. Excess Air Force assets can be located using DRMS.

33.4. Disposition of excess classified media. The ISSO or designated representative signs and affixes the appropriate disposition certification label and marks classified media as required according to the guidance in AFI 31-401 . Also, all personnel handling classified materials bear a responsibility to

ensure their media is appropriately marked. ***NOTE***: For your use, DLA has developed a label, based on the information required in ASD Memorandum, June 4, 2001. This is an optional form. Please note that it also contains a block to check if you are turning in housings where the hard drive has been removed. This form can be printed on sticky labels, i.e., Avery 5164 or Pres-a-ply 30604 (reference AFSSI 5020 [FOUO] and AFI 31-401).

33.5. DELETED.

33.6. DELETED.

33.7. DELETED.

33.8. DELETED.

33.9. DELETED.

33.10. DELETED.

34. Obtaining Excess Resources. If the parent MAJCOM allows the use of excess IT to satisfy new requirements, the ECOs review excess redistribution programs and reports to determine if suitable excess resources are available.

34.1. The ECO may direct reutilization of IT assets to replace equipment that does not meet minimum standards when allowed by the parent MAJCOM.

34.2. To acquire equipment from the DRMO, the EC submits documentation (DD Form 1348A-1, **Issue Release/Receipt Document**) for coordination to the ECO. Assets can either be viewed at the DRMO location or researched at **http://www.drms.dla.mil/rtda/**.

34.3. ECOs establish accountability in the AIM for IT hardware equipment acquired through any source that meets the criteria for accountability in paragraph **22.1.**

35. Transferring Excess Information Technology (IT) Systems Assets to the Defense Reutilization Marketing Office (DRMO).

35.1. DRMO is the primary source for disposal of all military property and equipment. All Air Force IT (accountable or non-accountable) when practical, should be disposed of through the DRMO.

35.2. DRMO guidelines for excess and the disposal of IT assets can be found at **http://www.drms.dla.mil/rtd03/dodit.htm**.

35.3. All hard drives for IT assets being disposed of or transferred to DRMO within or outside of the DOD will be sanitized (i.e. overwriting, degaussing, or destroying) according to AFSSI 5020 (FOUO).

35.4. ECO's must establish a MOA with their servicing DRMO in order to transfer IT equipment directly to local schools under the Computers for Learning Program. Donations of IT equipment to schools can only take place AFTER completion of the mandatory DOD reutilization screening and then the IT equipment may be donated only to registered and qualified institutions identified by the DRMS.

35.4.1. The Air Force cannot donate IT assets directly to a school without the approval or knowledge of the DRMO.

35.5. The trade-in of Air Force IT assets is an allowable excess transaction under the provisions outlined in AFPD 23-5, *Reusing and Disposing Of Materiel*, as long as the transaction results in measurable savings to the Air Force. Additional guidance regarding equipment exchanges related to credit or warranty action is addressed in AFMAN 23-110, Volume 2, Part 13, Chapter 8.

35.5.1. Adherence to remanence security requirements is vital to all transactions relating to excess IT, whether they are credit or warranty exchanges or direct disposals to the DRMO.

36. DELETED.

37. DELETED.

38. Information Collections, Records, and Forms and Information Management Tools (IMT).

38.1. Records. Records generated are maintained according to AFRIMS RDS located at **https://afrims.amc.af.mil/rds_series.cfm**.

38.1.1. AIM: use Table 33-7, Rule 8 disposition schedules to delete/dispose of information.

38.1.2. Completed Checklist (AF Form 2519): use Table 37-15, Rule 31.

38.1.3. IT Inventory: use Table 33-7, Rule 12; and cannibalizations (Spare parts) records: use Table 23-3, Rule 6.

38.2. Forms or IMTs (Adopted and Prescribed):

38.2.1. Adopted Forms or IMTs. DD 200, **Financial Liability Investigation of Property Loss**; and DD Form 1149, **Requisition and Invoice/Shipping Document**; DD Form 1348A-1, **Issue Release/Receipt Document**; AF IMT 847, **Recommendation for Change of Publications**; AF IMT 2519, **All Purpose Checklist**;

38.2.2. Prescribed Forms or IMTs. AF IMT 597, **ADPE Maintenance Record**.

JOHN L. WOODWARD, JR., Lt Gen, USAF
DCS/ Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

PL 104-52, *Telephone Installation and Charges*, page 109 STAT 468, Section 620 (31 U.S.C. 1348)

E.O. 12999, *Education Technology: Ensuring Opportunity for All Children in the Next Century*

ASD Memorandum, Disposition of Unclassified DOD Computer Hard Drives, June 4, 2001: **http://www.drms.dla.mil/turn-in/#harddrive**

DODD 8000.1, *Management of DOD Information Resources and Information Technology*, February 27, 2002, with Change 1, March 20, 2002

DODD 8100.1, *Global Information Grid (GIG) Overarching Policy*, September 19, 2002

DODI 4100.33, *Commercial Activities Program Procedures*, September 9, 1985, with Change 3, October 6, 1995

DODI 5000.64, *Defense Property Accountability*, August 13, 2002

DODI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

DOD 4140.1-R, *DOD Supply Chain Materiel Management Regulation*, May 23, 2003

DOD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4, August 6, 1998

DOD 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, January 2002

AFPD 10-6, *Mission Needs and Operational Requirements*

AFPD 23-5, *Reusing and Disposing Of Materiel*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems* (will become Information Resources Management)

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFPD 65-2, *Management Control Program*

AFI 10-1401, *Modernization Planning Documentatio*n

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*

AFI 21-116, *Maintenance Management of Communications-Electronics*

AFI 23-111, *Management of Government Property in Possession of the Air Force*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-104*, Base-Level Planning and Implementation*

AFI 33-114, *Software Management*

AFI 33-115, Volume 1, *Network Operations (NETOPS)*

AFI 33-202, Volume 1, *Network and Computer Security*

AFI 63-124, *Performance-Based Service Contracts (PBSC)*

AFI 65-501, *Economic Analysis*

AFMAN 23-110, *USAF Supply Manual*

AFMAN 23-220, *Reports of Survey for Air Force Property*

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

AFSSI 5020, (FOUO) *Remanence Security*

AFWay Users Guide

FAR 7.5, *Inherently Governmental Functions*

FAR 45.505, *Records and Reports of Government Property*

DFAR Supplement, Part 217.70, *Exchange of Personal Property*

Uniform Code of Military Justice

FPM Letter 368-1, 26 March 1991, Federal Flexible Workplace Project

Technical Order 00-20-2, *Maintenance Data Documentation*

AFRIMS RDS (**https://afrims.amc.af.mil/rds_series.cfm**)

Federal Financial Accounting Standards No.6, dated 1996

Abbreviations and Acronyms

AF—Air Force (used on forms only)

AFEMS—Air Force Equipment Management System

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRIMS—Air Force Records Information Management System

AFSSI—Air Force Systems Security Instruction

AFWay—Air Force Way

AIM—Asset Inventory Management

AIS—Automated Information System

ANG—Air National Guard

ASD—Assistant Secretary of Defense

C4—Command, Control, Communications, and Computer

C-E—Communications- Electronics

CBT—Computer Based Training

CPU—Central Processing Unit

CSA—Client Support Administrator

CSM—Computer Systems Management

CSMWG—Computer Systems Management Working Group

CSO—Communications and Information Systems Officer

DAA—Designated Approving Authority

DD—Department of Defense (used on forms only)

DFAR—Defense Federal Acquisition Regulation

DFAS—Defense Finance and Accounting Service

DLA—Defense Logistics Agency

DOD—Department of Defense

DRA—Defense Reporting Activity

DRMO—Defense Reutilization and Marketing Office

DRU—Direct Reporting Unit

E.O.—Executive Order

E-mail—Electronic Mail

EA—Economic Analysis

EC—Equipment Custodian

ECO—Equipment Control Officer

FAR—Federal Acquisition Regulation

FOA—Field Operating Agency

FOB—Found-On-Base

GO—General Officer

HTSA—Host Tenant Support Agreement

HQ AETC—Headquarters Air Education and Training Command

HQ AFCA—Headquarters Air Force Communications Agency

HQ OSSG—Headquarters Operations and Sustainment Systems Group

HQ SSG—Headquarters Standard Systems Group

IA—Information Assurance

ISSO—Information Systems Security Officer

IT—Information Technology

MAJCOM—Major Command

MECO—Major Command Equipment Control Officer

MOA—Memorandum of Agreement

MSG—Material Systems Group

NCO—Noncommissioned Officer

OPR—Office of Primary Responsibility

PA—Program Agreement

PBSC—Performance Based Service Contracts

PC—Personal Computer

PDA—Personal Digital Assistant

PL—Public Law

PM—Program Manager

PMO—Program Management Office

RDS—Records Disposition Schedule

ROS—Report of Survey

SAF—Secretary of the Air Force

SES—Senior Executive Service

USAF—United States Air Force

Terms

Accountable Officer—An individual appointed by proper authority who maintains items and/or financial records in connection with government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or care and safekeeping. In all cases, the accountable officer is responsible for establishing and maintaining financial property control records, controlling the processing of supporting documentation, and maintaining supporting document files. The primary accountable officers under the Air Force ROS System include: chief of supply, medical supply officer, munitions officer, fuels officer, communications and information systems officer, civil engineer, etc.

Cannibalization—Authorized removal of a specific assembly, subassembly or part from one system for installation on another end item to satisfy an existing supply requisition and to meet priority mission requirements with an obligation to replace the removed item. Canning is the act of removing serviceable parts from one IT system for installation in another IT system when removal of parts will cause the first system to not perform as designed.

C-E Maintenance—Any action taken to restore C-E equipment to operational status, to perform preventive maintenance inspections on C-E equipment, or to install or remove C-E equipment.

C-E Equipment—All communications systems and equipment including but not limited to ground-based radio and wireless systems including infrared; radar, meteorological and navigational radiation aids used for aircraft control and landing; radiating aids for fire control; imagery, video processing equipment and

intrusion detection systems, satellite, microwave and telemetry equipment; mission critical computer hardware, telecommunications switching equipment, cable and antenna systems; cryptographic equipment and communications consoles; and electronic counter-measures and related radiation, re-radiation, and electronic devices.

Central Processing Unit (CPU)—The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Client Support Administrator (CSA)—The primary point of contact for computer related problems. The person appointed and certified under AFI 33-115, Volume 1 to support information systems/ technology related tasks. Formerly Workgroup Manager (WM).

Command, Control, Communications, and Computer (C4) System—An integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all phases of the operational continuum. This system includes visual information support systems. Within the Air Force referred to as communications and information systems.

Communications and Information Systems Officer (CSO)—The term CSO identifies the supporting systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol SC that is expanded to three and four digits to identify specific functional areas. CSOs are accountable officers for all automated data processing equipment in their inventory.

Computer System—A functional unit, consisting of one or more computers and associated software, that (1) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; (2) executes user-written or user-designated programs; and (3) performs user-designated data manipulation, including arithmetic and logic operations. ***NOTE:*** A computer system is a stand-alone system or may consist of several interconnected systems. Personal computers, microcomputers, minicomputers, multi-user systems, all standard multi-user small computer requirements contract systems, text processors, word processors, intelligent typewriters, and workstations are examples of computer systems.

Department of Defense (DOD) Redistribution Program—Worldwide program, initiated by DOD for reporting, screening, redistributing, and disposing of automation resources that have become excess under an original application.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an information system or network within a specified environment. (AFI 33-202, Volume 1)

Documentation—The formal standardized recording of detailed objectives, policies, and procedures governing conception, authorization, design, testing, implementation, operation, maintenance, modification, and disposition of data administration techniques and applications.

Economic Analysis (EA)—An EA helps us make rational choices among competing alternatives. A good EA systematically examines and tells us about costs, benefits, and risks of various alternatives.

Equipment Control Officer (ECO)—An individual appointed by the applicable CSO to manage and control IT assets resources for a base. (***NOTE:*** A tenant unit may have its own ECO. This should be coordinated among the main base Communications unit, the tenant unit, and the MAJCOM of the tenant unit.)

Equipment Custodian (EC)—An individual who acts as a subordinate to the applicable ECO and performs inventory, utilization, and maintenance recording and reporting and other custodial duties as the ECO requires.

Hardware—(1) The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. (2) In data automation, the physical equipment or devices forming an IT system and peripheral components. See also **software**.

Information Systems Security Officer (ISSO)—Official who manages the computer security program for an information system assigned to him or her by the Information Systems Security Manager; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. (***NOTE:*** See DODI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003.) An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DOD information system or organization. While the term IAO is favored within the DOD, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer). (AFI33-202, Volume 1).

Information Technology (IT)—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DOD component. For the purposes of the preceding sentence, equipment is used by a DOD component if the equipment is used directly or is used by a contractor under a contract with the DOD component that (1) requires the use of such equipment; or (2), requires the use to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (See DOD Directive 8000.1, *Management of DOD Information Resources and Information Technology*, February 27, 2002, with Change 1, March 20, 2002.) ***NOTE***: The focus of this instruction is IT hardware management. AFI 33-114 is the governing Air Force instruction for software.

Joint Service System—A standard system implemented at one or more services sites (U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine Corps). Systems acquisition, development, maintenance, and life-cycle support are assigned to a program manager assigned to one of the services.

Life-Cycle Management—(1) The management of a system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. (2) A management process, applied throughout the life of an AIS that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS.

Maintenance—(1) All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (2) All supply and repair action taken to keep a force in condition to carry out its mission. (3) The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or other real property) in such condition that it is continuously utilized, at its original or designed capacity and efficiency, for its intended purpose. (4) The function of keeping C4 items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors.

Major Command Equipment Control Officer (MECO)—The individual appointed by the CSO that oversees the management and control IT assets for the MAJCOM, FOA, and DRU.

Peripheral—Any equipment that provides the IT system with additional capabilities distinct from the central processing unit (e.g., a printer, mouse, disk drive, digitizer, etc.).

Pilferable—Items having a ready resale value, civilian utility or application, and therefore are especially subject to theft. Consideration must be given to the cost to provide controlled storage and handling compared to the potential losses when selecting items to be treated as pilferable items. Generally an item should not be coded for worldwide treatment as pilferable, unless the unit cost exceeds $100 and repetitive losses indicate the item is subject to theft; however, the unit cost criteria may be waived when management determines that losses on an item warrant the cost of additional controls.

Resources—Any IT system, component hardware and software, contractual services, personnel, supplies, and funds.

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Software—(1) A set of IT assets programs, procedures, and associated documentation concerned with the operation of an IT system (i.e., compilers, library routines, manuals, circuit diagrams). (2) The programs, procedures, rules, and any associated documentation pertaining to the operation of data processing systems.

System—A set of IT components and their external peripherals and software interconnected with another set. Typical systems include notebook computers, desktop PCs, networked and distributed systems (e.g., servers, workstations, data management processors, etc.), mainframe and midsize computers and associated peripherals.

Systems Administrator—The organization focal point for multi-user systems.

Attachment 2

DELETED

Attachment 3

INFORMATION TECHNOLOGY (IT) SYSTEMS CHECKLIST

Table A3.1. Questions for Information Technology (IT) Systems Checklist.

#	ITEM	REFERENCE	Y	N	NA
	Equipment Control Officer (ECO)				
1	Is a copy of AFI 33-112 available?				
2	Has the CSO appointed a primary and alternate ECO in writing? Does the selected individual meet the criteria as noted in AFI 33-112?	AFI 33-112, paragraphs **6.12.** and **10.1.**			
3	Does the ECO receive all computer systems, ensuring accountability and completion of all necessary documentation?	AFI 33-112, paragraph **10.2.1.** and **22.1.**			
4	Does the ECO account for IT, according to AFI 33-112, utilizing AIM?	AFI 33-112, paragraph **10.2.**			
5	Is the ECO accountable for equipment listed in their assigned AIM account?	AFI 33-112, paragraph **10.2.2.**			
6	Does the ECO assist the EC in determining ownership of all FOB IT assets and takes appropriate action to ensure accountability?	AFI 33-112, paragraph **10.2.3.**			
7	Does the ECO direct all ECs to conduct an annual physical inventory of assigned computer systems?	AFI 33-112, paragraph **10.2.5.**			
8	Does the ECO ensure completion of the annual physical inventory and that EC appointments are renewed annually?	AFI 33-112, paragraphs **10.2.5.**			
9	Does the ECO prepare AIM bar code labels and provide them to the EC as needed?	AFI 33-112, paragraph **10.2.10.**			
10	Does the ECO work with the EC to update the inventory as dictated by a ROS?	AFI 33-112, paragraph **10.2.29.**			
11	Does the ECO complete out-processing for departing ECs upon transfer of account and receipt of new appointment letters?	AFI 33-112, paragraph **10.2.12.**			
12	Does the ECO provide guidance and training for the ECs?	AFI 33-112, paragraph **10.2.13.**			
13	Does the ECO receive guidance and direction from the MECO?	AFI 33-112, paragraph **10.2.14.**			

#	ITEM	REFERENCE	Y	N	NA
14	Does the ECO correctly code deployed computer systems in AIM as directed by HQ USAF or MAJCOM and authorized by the applicable CSO?	AFI 33-112, paragraph **10.2.16.**			
15	Does the ECO attempt to reutilize excess organizational IT assets that meet minimum architecture standards before offering equipment to organizations outside the DRA, when allowed by the parent MAJCOM?	AFI 33-112, paragraph **10.2.18.**			
16	Does the ECO works with any tenant ECO to establish a host tenant agreement identifying any assistance required, such as AIM connectivity?	AFI 33-112, paragraph **10.2.25.**			
17	Does the ECO coordinate on all host tenant agreements?	AFI 33-112, paragraph **10.2.28.**			
	Equipment Custodian (EC)				
18	Are ECs and alternates appointed in writing by the organizational commander?	AFI 33-112, paragraph **7.5.**			
19	Are ECs responsible for all assigned IT hardware assets?	AFI 33-112, paragraph **11.1.**			
20	Do the ECs perform an annual physical inventory of all items in the account? Upon completion, does the EC and the organizational commander or equivalent sign the inventory with the original copy retained by the EC and a copy for the ECO file?	AFI 33-112, paragraph **11.1.1.**			
21	Does the EC ensure all accountable IT hardware equipment has an AIM bar code label attached when practical?	AFI 33-112, paragraph **11.2.**			
22	Does the EC obtain approval and coordinate all potential transfers of computer systems between accounts with the applicable ECO? ***NOTE***: ECs have no authority to transfer computer systems outside their account.	AFI 33-112, paragraph **11.3.**			
23	Does the EC sign for new equipment received through the ECO?	AFI 33-112, paragraph **11.5.**			
24	Does the EC provide appropriate documentation to the applicable ECO to clear the account of equipment that was shipped to another base/location, transferred to another account, donated to a school, or turned-in to DRMO?	AFI 33-112, paragraph **11.7.**			
25	Has a joint physical inventory been accomplished prior to equipment account transfer?	AFI 33-112, paragraph **11.10.**			

#	ITEM	REFERENCE	Y	N	NA
26	Does the EC out-process through the applicable ECO?	AFI 33-112, paragraph **11.9.**			
27	Does the EC initiate the ROS process according to AFMAN 23-220, concerning any lost, damaged, or destroyed IT assets?	AFI 33-112, paragraph **11.12.**			
28	Does the EC provide the applicable ECO a serialized numbered list of deployed IT assets?	AFI 33-112, paragraph **11.14.**			
29	Does the EC receive and secure all IT assets, if not received by the ECO, until proper accountability is established?	AFI 33-112, paragraph **11.15.**			

Attachment 4

IC 2001-1 TO AFI 33-112,
COMPUTER SYSTEMS MANAGEMENT

25 FEBRUARY 2001

SUMMARY OF REVISIONS

This change incorporates Interim Change (IC) 2001-1 (**Attachment 4**). It transfers the responsibility for purchasing and equipment accountability of general officers (GO) and senior executive service (SES) notebook computers to the base/local-level communications unit. Paragraph **3.** has been deleted and all information pertaining to the responsibilities of the Air Force Communications and Information Center (AFCIC) have been incorporated into paragraph **1.** See last attachment of this publication, IC 2001-1, for the complete IC. A (|) indicates revision from the previous edition.

1.3. Resolves operational issues on computer systems (HQ USAF/SCMOS).

1.4. Acts as the functional manager for the information processing management system (IPMS) and the Air Force Computer Systems Redistribution Program (HQ USAF/SCMOS).

1.5. Reviews policy and procedural recommendations to CSM processes (HQ USAF/SCMOS).

1.6. Ensures appropriate action is taken upon receipt of excess equipment requests.

1.7. Establishes a new defense reporting activity account (DRA) upon request of the major command equipment control officer (MECO) and receipt of appropriate information.

1.8. Reviews concerns expressed by MECOs about inclusion and, or exclusion of computer systems in IPMS.

1.9. Includes DRA information received from MECOs and adds to automation resources management system (ARMS) database.

1.10. Serves as Air Force focal point to Defense Information Systems Agency (DISA) concerning questions and, or comments pertaining to Assistant Secretary of Defense (ASD) Memorandum dated September 8, 1994, Subject: Interim Management Guidance on Defense Automation Resources Management; and Defense Automation Resource Management Manual, September 1988.

1.11. Establishes an Air Force computer system management working group (CSMWG) to support CSM personnel at all levels in the execution of their responsibilities as outlined in this instruction and other CSM-related guidance.

1.11.1. The CSMWG will include broad representation of CSM functions allowing for improved cross-feed of information and feedback from the field necessary to make informed decisions about CSM policy and procedures.

1.11.2. The CSMWG will:

1.11.2.1. Assist HQ USAF/SCMOS to resolve current or anticipated CSM-related issues whether technical, managerial, or administrative.

1.11.2.2. Assist HQ USAF/SCMOS to take functional improvement opportunity.

1.11.2.3. Serve as the Air Force CSM infrastructure to deal with CSM-related issues.

1.11.2.4. Identify CSM functional requirements and provide configuration control for automated information systems (AIS) dedicated to Air Force CSM.

3. DELETED.

20. (DOES NOT APPLY TO ANG) General Officers (GO) and Senior Executive Service (SES) Executives Computer Equipment.

20.1. Active duty GOs and SES', including brigadier general selects, are required to maintain e-mail contact with the Chief of Staff of the Air Force (CSAF). GO and SES computer requirements will be purchased through the local communications unit by the GO's or SES' current unit of assignment and will follow the standard requirement process. If the GO or SES desires, the computer may accompany the GO or SES from assignment to assignment. When the GO and SES decide to take their computer, they will work with the losing and gaining communications unit to ensure proper equipment inventory accountability. The local equipment custodian will retain accountability for the computer until transferred to the new location.

20.1.1. The local or supporting communications unit is responsible for setup/configuration, technology refreshment, hardware/software maintenance, and equipment accountability.

20.1.2. When a GO or SES retires or leaves Air Force service, the GO or SES must turn in the notebook computer to the local CSO.

20.1.3. DELETED.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 104-52, Telephone Installation and Charges (31 U.S.C. 1348)

Federal Personnel Manual System, FPM Letter 368-1 dated 26 March 1991, Subject: Federal Flexible Workplace Project

ASD Memorandum dated 8 September 1994, Subject: Interim Management Guidance on Defense Automation Resource Management

Defense Resource Management Manual, September 1988

The Privacy Act of 1974

Uniform Code of Military Justice

DoD 5200.28-M, *ADP Security Manual*, January 1973, with Change 1

DoD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4 dated August 6, 1998

AFPD 10-6, *Mission Needs and Operational Requirements*

DELETED AFPD 23-1, *Requirements and Stockage of Materiel* (not used in publication)

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 33-2, *Information Protection*

AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*

AFI 23-111, *Management of Government Property in Possession of the Air Force*

AFI 31-601, *Industrial Security Program Management*

DELETED AFI 33-102, *Command, Control, Communications, Computers, and Intelligence (C4I) Capabilities Planning Process* (rescinded 9 Aug 2000)

AFI 33-103, *Requirements Development and Processing*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-114, *Software Management*

AFI 33-115V1, *Network Management* (formerly AFI 33-115)

AFI 33-202, *Computer Security* (formerly AFSSI 5102)

AFI 33-203, *Emission Security*

AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322V4)

AFI 63-124, *Performance-Based Service Contracts (PBSC)* (formerly AFMAN 64-108)

AFR 177-106, *Materiel and Property Accounting* (will convert to DFAS-DE7420.1-R)

AFCAT 36-2223, *USAF Formal Schools*

AFIND 5, *Numerical Index of Specialized Information Protection/Assurance Publications*

AFSSM 7011, *Emission Security Countermeasures Reviews* (will convert to AFMAN 33-214V2)

Abbreviations and Acronyms

ACC— Air Combat Command

ADPE— Automated Data Processing Equipment

AETC—Air Education and Training Command

AF— Air Force (used on forms only)

AFCAT—Air Force Catalog

DELETED AFCIC— Air Force Communications and Information Center (no longer exists)

AFGOMO—Air Force General Officer Matters Office

AFI— Air Force Instruction

AFIND— Air Force Index

AFMAN— Air Force Manual

AFPCA—Air Force Pentagon Communications Agency

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

AFSSI —Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

AFTMS—Air Force Training Management System

AIS—Automated Information System

ANG—Air National Guard

ANGIND—Air National Guard Index

ARMS—Automation Resources Management System

ASD—Assistant Secretary of Defense

C4—Command, Control, Communications, and Computer

CPU —Central Processing Unit

CSM—Computer Systems Management

CSMWG—Computer System Management Working Group

CSO—Communications and Information Systems Officer

CSSO—Computer Systems Security Officer

DAA—Designated Approval Authority

DAP —Data Automation Plan

DAR—Data Automation Requirement

DD—Department of Defense (used on forms only)

DDN—Defense Data Network

DFAS—Defense Finance and Accounting Service

DISA—Defense Information Systems Agency

DISN —Defense Information Systems Network

DoD—Department of Defense

DRA—Defense Reporting Activity Account

DRMO—Defense Reutilization and Marketing Office

EC— Equipment Custodian

ECO—Equipment Control Officer

EMSECEmission Security

FOB Found-On-Base

DELETED FPI—Functional Process Improvement (not used in publication)

GLSA—General Ledger Subsidiary Account

GO —General Officer

GSA—General Services Administration

HQ AETC—Headquarters Air Education and Training Command

HQ AFCA—Headquarters Air Force Communications Agency

HQ SSG—Headquarters Standard Systems Group

HQ USAF—Headquarters United States Air Force

IC— Interim Change

IMPAC—International Merchant Purchase Authorization Card

IP —Information Protection

IPMS—Information Processing Management System

DELETED IRCN—Interagency Report Control Number (not used in publication)

LAN—Local Area Network

LRU—Line Replaceable Unit

MAC —Major Command Code

MAJCOM—Major Command

MECO—Major Command Equipment Control Officer

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

NCC—Network Control Center

NIPRNET—Non-Classified Internet Protocol Network

OCM—Organization Computer Manager

OCONUS—Outside the Continental United States

OPR—Office of Primary Responsibility

PC— Personal Computer

PCS— Permanent Change of Station

PM—Program Manager

PMO—Program Management Office

DELETED POM—Program Objective Memorandum (not used in publication)

ROS—Report of Survey

SA —Systems Administrator

SCIF—Sensitive Compartmented Information Facility

DELETED SE—Senior Executive (not used in publication)

SES— Senior Executive Service

SF —Standard Form

UCMJ—Uniform Code of Military Justice

UTC—Unit Type Code

Terms

Air Force Infrastructure Support Contracts— Contracts that provide small computer resources at discount prices, and a standard structure for Air Force-wide interoperability with other small computers (formerly known as Air Force computer requirements Contracts, Indefinite Delivery/Indefinite Quantity, and Requirements Contracts)

Cannibalization— The act of removing serviceable parts from one computer system for installation in another computer system when removal of parts will cause the first system to not perform as designed.

Central Processing Unit (CPU)— The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Command, Control, Communications, and Computer (C4) System— An integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, through all phases of the operational continuum. This system includes visual information support systems. Within the Air Force referred to as Communications and Information systems.

Communications and Information Systems Officer (CSO)— The term CSO identifies the supporting systems officer at all levels. At base level, this is the commander of the communications unit responsible for carrying out base Comm and Info systems responsibilities. At MAJCOM, and other activities responsible for large quantities of Comm and Info systems, it is the person designated by the commander as responsible for overall management of systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol SC that is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officer for all automated data processing equipment in their inventory.

Computer System— A functional unit, consisting of one or more computers and associated software, that (a) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; (b) executes user-written or user-designated programs; and (c) performs user-designated data manipulation, including arithmetic and logic operations. NOTE: A computer system may be a stand-alone system or may consist of several interconnected systems. Personal computers, microcomputers, minicomputers, multi-user systems, all standard multi-user small computer require-

ments contract systems, text processors, word processors, intelligent typewriters, workstations, are examples of computer systems.

Department of Defense (DoD) Redistribution Program — Worldwide program, initiated by DoD for reporting, screening, redistributing, and disposing of automation resources that have become excess under an original application.

Designated Approval Authority (DAA)— The organization or individual that establishes necessary procedures and controls to protect information and ensures the availability and integrity of critical processes. Refer to AFSSI and AFSSM 5000-series publications for additional information.

Documentation— The formal standardized recording of detailed objectives, policies, and procedures governing conception, authorization, design, testing, implementation, operation, maintenance, modification, and disposition of data administration techniques and applications. All DoD computer systems documentation is written in accordance with DOD Instruction 7935.1-2.

Emission Security (EMSEC)— Short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

Equipment Control Officer (ECO)— An Individual appointed by the applicable communications-information systems officer to manage and control computer systems resources for a base. (NOTE: MAJCOMs may appoint a tenant ECO to provide computer systems control and accountability for their tenant units.)

Equipment Custodian (EC)— An individual who acts as a subordinate to the equipment control officer (ECO) and performs inventory, utilization, and maintenance recording and reporting and other custodial duties as the ECO requires.

Hardware— 1. The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. 2. In data automation, the physical equipment or devices forming a computer and peripheral components. See also software.

Joint Service System— A standard system implemented at one or more services sites (U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine Corps). System acquisition, development, maintenance, and life-cycle support are assigned to a program manager assigned to one of the services.

Life-Cycle Management— The management of a system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. 2. A management process, applied throughout the life of an automated information system (AIS), that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS.

Line Replaceable Unit (LRU)— A module, subassembly, or printed circuit card you can replace or repair without soldering.

Maintenance — 1. All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. 2. All supply and repair action taken to keep a force in condition to carry out its mission. 3. The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility sys-

tem, or other real property) in such condition that it may be continuously utilized, at its original or designed capacity and efficiency, for its intended purpose. 4. The function of keeping (C4) items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors.

Major Command Equipment Control Officer (MECO)— The individual appointed by the major command (MAJCOM) communications and information systems officer to manage and control computer systems resources for a MAJCOM.

Network Control Center (NCC)— The base focal point for network management, problem resolution and, computer maintenance issues (formerly known as Base Network Control Center [BNCC]).

Peripheral — Any equipment that provides the computer with additional capabilities distinct from the central processing unit. Examples are a printer, mouse, disk drive, digitizer, etc.

Protocol—In data communications, (a) a set of rules governing network functionality. The open system interconnection reference model uses sets of communication protocols to facilitate communications between computer networks and their components, or (b) a formally specified set of conventions governing the format and control of inputs and outputs between two communicating systems.

Resources—Any computer system, computer system component hardware and software, contractual services, personnel, supplies, and funds.

Shareware—Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Software— 1. A set of computer systems programs, procedures, and associated documentation concerned with the operation of a computer system (i.e., compilers, library routines, manuals, circuit diagrams). 2. The programs, procedures, rules, and any associated documentation pertaining to the operation of data processing systems.

System— A computer system and its external peripherals and software interconnected with another computer system. Typical "systems" include laptop personal computer (PC), desktop PCs, networked and distributed computer systems (e.g., servers, workstations, data management processors, etc.), mainframe and "midsize" computers and associated peripherals.

Systems Administrator— The organization focal point for multiuser systems.

Wing Information Protection (IP) Office—Office that administers the wing IP program, advises the base computer systems security officer, and acts as the accreditation advisor to the designated approving authority. The office is within the wing communications unit.

Attachment 5

EQUIPMENT STATUS REPORTING

A5.1. The status codes in **Table A5.1.** describe the operational status of a component or DRA. Valid values are:

Table A5.1. IT asset status codes for equipment status reporting.

Status Code	Status Description
01	Programmed, planned, or unapproved order.
02	Approved acquisition, or on order.
03	Received on-site, but not installed.
04	Undergoing acceptance testing, during installation.
11	Installed, accepted, and in use.
12	Available excess.
41	Discontinued use.
52	Transferred in from another DRA.
	Operational spare—backup/safety item available to prevent critical failures to network/system. ***NOTE:*** At the time of publication, the AIM system could not be updated to reflect this status code due to funding limitations. Until the system is updated, users may use the Remarks field in AIM to annotate an asset as an operational spare.

Attachment 6

INTERIM CHANGE (IC) 2006-1 TO AFI 33-112, COMPUTER SYSTEMS MANAGEMENT

7 APRIL 2006

INFORMATION TECHNOLOGY HARDWARE ASSET MANAGEMENT

This Air Force instruction (AFI) implements Air Force Policy Directives (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; 33-2, *Information Protection* (will become *Information Assurance*); and 10-6, *Mission Needs and Operational Requirements*; by identifying responsibilities for supporting Air Force information technology (IT) equipment (computer systems). Some paragraphs in this instruction that do not apply to non-Air Force-managed joint service systems, are marked *(NOT APPLICABLE TO NON-AIR FORCE-MANAGED JOINT SERVICE SYSTEMS)*. This instruction applies to Air National Guard (ANG). Refer technical questions about this instruction to Headquarters Air Force Communications Agency (HQ AFCA/EVPS), 203 West Losey Street, Room 3065, Scott AFB IL 62225-5222. Send recommended changes or comments to HQ AFCA/EASD, 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using Air Force (AF) IMT 847, **Recommendation for Change of Publication**, with an information copy to the Office of the Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Director of Information, Services and Integration (SAF/XCI), 1250 Air Force Pentagon, Washington DC 20330-1250. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records,* (will become AFMAN 33-363) and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds_series.cfm**. See **Attachment 1** for a glossary of references and supporting information. **Attachment 2** contains an address listing of key organizations. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF REVISIONS

This change incorporates interim change IC 2006-1 (**Attachment 6**). It changes the name to *Information Technology Hardware Asset Management*. The main focus is to expand information technology (IT) asset management focus from computer system management to IT hardware asset management, remove all references to the Information Processing Management System (IPMS) and add references to the Asset Inventory Management (AIM) module of the Air Force Equipment Management System (AFEMS). It also incorporates numerous office symbol changes to reflect Secretary of the Air Force (SAF/XCI), HQ USAF/ILC, HQ USAF/CIO, HQ USAF/XI, Headquarters Standard System Group (HQ SSG), and AFCA transformation. Paragraph **1.** is changed to reflect SAF/XCI instead of Headquarters United States Air Force (HQ USAF/SC) and further define responsibilities of the Air Force Computer Systems Management Working Group (CSMWG). Paragraph **2.** is changed to define SAF/AAZ's cognizance over networks processing Special Access Program/Special Access Required information. Paragraph **3.** defines AFCA responsibilities. Paragraph **4.** is changed to update the training responsibilities of Headquarters Air Education and Training Command (HQ AETC). Paragraph **5.** is modified to change program management of the Air Force IT asset management system from HQ SSG to the Headquarters Operations and Sustainment Systems Group (HQ OSSG) and removes references to IPMS. Paragraph **6.** changes to the responsi-

bilities of the Communications and Information Systems Officer (CSO). Paragraph **6.12.** is changed to provide detailed criteria for appointing the primary and alternate equipment control officer (ECO). Paragraph **7.** updates the organizational commander's duties. Changes include the requirement for the commander to sign the annual inventory listing and detailed criteria for appointing equipment custodians. Paragraph **7.14.** is deleted. Paragraph **7.15.**was added to ensure compliance with the Department of Defense (DOD) policy for disposition of computer hard drives. Paragraph **8.** is deleted. The organization computer manager responsibilities previously defined in paragraph **8.** are performed by Client Support Administrators (CSA). Guidance for CSAs is found in AFI 33-115, Volume 1, *Network Operations (NETOPS)*. Paragraph **9.** removes references to IPMS and defines the grade requirements and appointing official for the major command equipment control officer (MECO). Paragraph **10.** removes references to IPMS, updates ECO responsibilities, and clarifies inventory procedures. Paragraph **10.** also requires the ECO to update the asset status in AIM upon receipt of IT hardware assets. Paragraph **11.** updates equipment custodian responsibilities. Paragraph **11.1.1.** requires the commander's signature in the AIM inventory listing. Paragraph **11.16.** is added to direct the equipment custodian (EC) to coordinate with the Information Systems Security Officer (ISSO) for hard drive sanitation according to the procedures outlined in Air Force Systems Security Instruction (AFSSI) 5020 (FOUO), *Remanence Security*. Paragraph **12.** is deleted. Paragraph **13.** is deleted. Paragraph **14.** directs users to refer to AFI 33-202, Volume 1, *Network and Computer Security*. Paragraphs **14.1.**, **14.2.**, and **14.3.** are deleted. Paragraph **15.** is expanded to define Air Force contractor responsibilities for funding, accountability and Chief Financial Officer reporting. Paragraph **16.** removes references to IPMS and changed to Acquisition of Information Technology (IT) Assets. Paragraph **16.1.** makes procurement of desktops and laptops through Air Force Way (AFWay) mandatory unless waived by the major command (MAJCOM) Chief Information Officer (CIO)/A6. Paragraphs **17.** and **18.** are deleted. Deployment considerations listed in paragraph **17.** are moved to paragraph **6.** under CSO responsibilities. Paragraph **19.** includes policy for use of all IT assets. Paragraph **19.2.** is added to instruct personnel not to input or store government information/data on privately-owned IT assets without approval of the Designated Approving Authority (DAA) according to AFI 33-202, Volume 1. Paragraphs **19.2.1.**, **19.2.2.**, **19.3.**, and **19.4.** are deleted. Paragraph **20.** is changed to include Personal Digital Assistants (PDA). Paragraph **21.** is changed to include procedures for the exchange or sale of government automated resources programs. Paragraph **22.** is changed to Inventory Management and Accountability of IT Hardware Assets. Paragraph **22.1.** is changed to provide a link on the Air Force Portal to a comprehensive and current list of accountable and non-accountable assets to help determine the accountability of IT assets. Paragraph **22.1.1.** is added to assign management and oversight of the official Air Force accountability list to the CSMWG. Paragraphs **23.**, **24.**, and **25.** are deleted. The requirement in paragraph **24.** to use labels for identification of IT assets is moved to paragraph **6.15.** Paragraph **26.** removes references to IPMS. Paragraph **27.** removes maintenance practices specific to computer systems and applies maintenance concepts for IT assets. Changes to paragraph **27.** also require the CSO to establish a Logistics Support Plan to ensure logistics support for IT assets throughout the expected lifecycle and offers methods to compute operational spares. Paragraph **28.** is deleted. Paragraph **29.** includes maintenance reporting for IT assets. Paragraphs **30.** and **31.** are deleted. Paragraph **32.** is changed to encompass IT assets instead of computer systems. Paragraph **33.** defines excess and implements procedures to dispose of excess through AIM. Changes also require IT assets picked up as excess to be accounted for in AIM. Cannibalization guidelines for spare parts are now included in paragraph **27.** Paragraph **34.** reflects procedures for obtaining excess IT assets in the AIM environment. Paragraph **35.** changes transferring excess IT assets to the Defense Reutilization Marketing Office (DRMO). References to the Computers for Learning Program and Executive Order (E.O.) 12999, *Education Technology: Ensuring Opportunity for All Children in the Next Century*, are also added to Paragraph **35.** Paragraphs **36.** and **37.** are deleted. Para-

graph **38.** adds reference to the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). **Attachment 1** is updated as a glossary of references and supporting information. **Attachment 2** is deleted. **Attachment 3** provides a checklist for IT assets and to comply with this IC. **Attachment 5** is added to show AIM asset status codes. A bar (|) indicates a revision from the previous edition.

1. Office of the Secretary of the Air Force for Warfighting Integration and Chief Information Officer, Director of Information, Services and Integration (SAF/XCI):

1.1. Develops, publishes, and disseminates Air Force doctrine and policy for information technology (IT) asset systems.

1.2. Identifies formal IT management training requirements.

1.3. Resolves management issues on IT hardware assets accounted for in the Asset Inventory Management (AIM) module and resolves policy disagreements between major commands (MAJCOM), functional managers, and non-Air Force agencies.

1.4. Acts as functional manager for the IT component of the Air Force Equipment Management System (AFEMS). The IT hardware component of the AFEMS is called the AIM module.

1.5. DELETED.

1.6. Sets policy and works in conjunction with Defense Logistics Agency (DLA/DRMS) on disposition of excess IT assets.

1.7. DELETED.

1.8. DELETED.

1.9. DELETED.

1.10. DELETED.

1.11. Establishes and chairs the Air Force Computer Systems Management Working Group (CSMWG) that directly supports CSM personnel at all levels including MAJCOM Equipment Control Officers (MECO), Communications and Information Systems Officers (CSO), Equipment Control Officers (ECO), organizational commanders and computer equipment custodians (EC) in the execution of their responsibilities as delineated in this instruction. The CSMWG provides broad representation allowing for improved cross feed of information and feedback from the field necessary to make informed decisions about CSM policy and procedures. The CSMWG serves as the Air Force CSM management infrastructure to deal with all CSM-related issues in an efficient and effective manner.

1.11.1. DELETED.

1.11.2.1. Develops proposed solutions on issues affecting IT system life-cycle management.

1.11.2.2. Identifies functional improvement opportunities for review, prioritizing, approval, and budgeting considerations.

1.11.2.3. Advises Air Force leadership on IT management issues.

1.11.2.4. Defines new functional requirements and provides oversight to automated information systems (AIS) processes supporting Air Force IT management.

1.11.2.5. Works with the IT Commodity Council on procurement initiatives.

1.12. Issues communications-electronics (C-E) maintenance management policy (see AFI 21-116, *Communications-Electronics Maintenance Management*). The intent of AFI 21-116 is to ensure only qualified personnel perform maintenance to avoid unnecessary risks to personnel and prevent damage to C-E equipment.

2. Administrative Assistant to the Secretary of the Air Force, Security and Special Programs Oversight (SAF/AAZ).

2.1. Provides policy and oversight on computer security pertaining to networks processing Special Access Program/Special Access Required information in their role as Special Access Program Coordination Office.

2.1.1. Air Force information technology assets, under the cognizance of the Special Access Program Coordination Office, may be tracked in the AIM module of AFEMS, if the cognizant security authority determines that there are no security concerns. SAF/AAZ provides guidance for meeting regulatory compliance for IT assets that are not tracked in AIM.

3. Headquarters Air Force Communications Agency (HQ AFCA).

3.1. Provides guidance and support to MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) in developing, implementing, and managing IT assets.

3.2. Reviews, evaluates, and interprets issues/problems and makes recommendations to SAF/XCII on policy changes.

3.3. Reviews, interprets, and disseminates Air Force policy.

3.4. Acts as office of primary responsibilities (OPR) for this instruction.

4. Headquarters Air Education and Training Command (HQ AETC).

4.1. Provides formal IT training when directed by SAF/XCI.

5. Headquarters Operations and Sustainment Systems Group (HQ OSSG/LRE).

5.1. Functions as Program Manager (PM) for the AIM module.

5.2. DELETED.

5.3. Submits the special year-end chief financial officer report to the Defense Finance and Accounting Service (DFAS).

5.4. Proposes technical solutions for defined requirements.

5.5. Coordinates all requirements and associated cost data through the program agreement (PA) manager for review and approval.

5.6. Notifies the PA manager of all unfunded requirements.

5.7. Coordinates software releases through the PA manager prior to scheduled release.

5.8. Provides input to program management reviews.

5.9. Completes required Information Support Plan/certification documentation prior to scheduled release.

5.10. Develops and maintains the AIM Computer Based Training (CBT) courseware and AIM User's Manual.

5.11. Provides operations, programming, and software support.

6.1. DELETED.

6.2.1. Ensure users and mission planners use strategy-to-task methodologies and the Air Force modernization planning processes to link IT investments to mission essential task improvements (see AFI 10-1401, *Modernization Planning Documentation*). The CSO integrates these requirements into the base Communications and Information Systems blueprint.

6.3. Is the accountable officer for all IT hardware equipment listed in their assigned AIM account. Ensures the AIM inventory is used to provide accountability of all base IT hardware resources assigned to that Defense Reporting Activity (DRA). Refer to paragraph **22.1.** to determine if a particular piece of IT hardware equipment should be accounted for using methods or systems other than AIM.

6.3.1. DELETED.

6.3.2. DELETED.

6.4. Assists in planning and execution of all activities related to the deployment of systems.

6.5. Assists the supporting contracting officers in developing an acquisition strategy for maintenance contracts.

6.5.2. DELETED.

6.6. Ensures identification and submission of maintenance requirements, performance work statements and surveillance plans (see AFI 63-124, *Performance-Based Service Contracts [PBSC]*).

6.7. DELETED.

6.8. Analyzes IT asset maintenance cost data to assist in developing cost-effective maintenance solutions.

6.8.1. Directs retention of serviceable excess IT assets, when allowed by the parent MAJCOM, for maintenance redundancy or operational spares, by ensuring use of sharing and redistribution programs to meet user requirements.

6.8.2. Authorizes removal/transfer of unserviceable IT assets for spare parts.

6.8.3. Authorizes cannibalization of IT assets to satisfy critical mission requirements. Maintenance actions to obtain assemblies, subassemblies, or parts from spare IT assets are considered transfers and will not be treated as cannibalization actions.

6.10. Coordinates action to ensure secure, climate controlled, and easily accessible facilities with sufficient floor space are provided to the equipment control officer (ECO) for receiving, storing, and distributing IT assets.

6.11. Coordinates on IT asset requirements with the appropriate office or unit.

6.12. Appoints primary and alternate ECOs and provides a copy of the appointment letter to the MECO. Although no grade restrictions apply for these positions, the primary and alternate ECOs should have the leadership skills and IT asset knowledge necessary to provide guidance and direction to the EC. The recommended minimum rank/grade requirement for the primary ECO is Technical Sergeant/GS-7. An airman (Senior Airman or below) may be appointed as an alternate ECO, if the CSO believes the airman is mature enough to handle the responsibility See paragraph **15.** for contractors. ***NOTE:*** The primary ECO will supervise the alternate ECO in performance of duties and responsibilities.

6.12.1. DELETED.

6.13. DELETED.

6.14. DELETED.

6.15. Where practical (e.g., due to size limitations) ensure mandatory AIM-generated standard product (bar code) labels are used to identify all IT assets within their DRA.

7. Organization Commanders or Equivalent. Commanders or their equivalent with IT assets are responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to IT assets under their control. The accountable officer is responsible for all IT assets within their organization.

7.4. Reviews assigned IT assets annually to determine if the IT is obsolete, still meets user requirements or needs modification and act accordingly.

7.5. Appoints, in writing, primary and alternate ECs, no later than 45 days prior to the projected departure of the current EC. According to AFMAN 23-110, Volume 2, Part 2, Chapter 22, ECs may be military (see note) or civilians. Contractors may also be ECs according to AFI 23-111, *Management of Government Property in Possession of the Air Force,* if the contract so stipulates and must be mutually agreeable to the organization commander and the CSO. This applies to active duty, guard, and reserve personnel. Foreign nationals or local wage rate employees (foreign nationals in host countries) may be appointed primary or alternate custodians only when they may be held pecuniary liable under the law of the host country. Organization commanders must review the provisions and restrictions outlined in AFI 31-501, *Economic Analysis*, AFI 33-202, Volume 1, *Network and Computer Security*, and AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, before appointing foreign nationals as primary or alternate equipment custodians. ***NOTE***: An airman (Senior Airman or below) may be appointed primary or alternate custodian by the organization commander, if the commander believes the airman is mature enough to handle the responsibility.

7.5.1. Sends the EC appointment letter and request for EC training to the ECO.

7.5.1.1. The EC appointment letter should be dated and contain the names of the primary and alternate ECs. The appointment letter should also contain the date the primary and alternate EC received training from the ECO.

7.5.1.2. Ensures the primary or alternate EC is scheduled for training with the ECO within 30 days of initial appointment and annually thereafter.

7.5.1.3. Annually reviews EC appointment letters and training dates to ensure the primary and alternate EC names are current and they have completed annual EC training. After the review, send a new EC appointment letter as described in paragraph **7.5.1.1.** to the ECO. When possible, the review should be held in conjunction with the annual inventory.

7.5.3. Ensures outgoing and incoming primary EC conduct and sign a loss-gain joint physical inventory and reconcile missing items under the guidance of the ECO, not later than 30 days prior to the primary EC being relieved of duty. In deployed locations, the forward commander will determine timeline for transfer of duties based on rotation schedules.

7.5.3.1. Refer to AFMAN 23-220, *Reports of Survey for Air Force Property*, to determine if a Report of Survey (ROS) is required when there are inventory discrepancies that cannot be resolved prior to the custodian departing.

7.6. Ensures the EC performs a complete and accurate annual inventory. After the annual inventory is complete, the Commander signs the inventory listing. The Commander's signature certifies to the ECO that the annual physical inventory is complete.

7.9. Develops and implements a documented process according to AFI 33-114, *Software Management*, to ensure that all software is free of viruses.

7.10. Ensures all accountable IT assets are reported to the ECO for inclusion in the AIM inventory.

7.12. DELETED.

7.13. DELETED.

7.14. DELETED.

7.15. Ensures compliance with the disposition of Department of Defense (DOD) computer hard drive policy cited in the Office of the Assistant Secretary of Defense (ASD) Memorandum, "Disposition of Unclassified DOD Computer Hard Drives," dated June 4, 2001, or hard drive sanitation in accordance with the procedures outlined in Air Force Systems Security Instruction (AFSSI) 5020 (FOUO). Find additional guidance at **http://iase.disa.mil/policy.html**.

8. DELETED.

9.1. The MAJCOM CSO or FOA/DRU equivalent appoints the MECO. Although no grade restrictions apply for this position, the MECO should have the depth and experience necessary to provide guidance and direction to the ECO. Recommend minimum grade be a senior non-commissioned officer (NCO)/ GS-9 for this position. When the MECO changes, the MAJCOM CSO notifies SAF/XCII (**safcxiiworkflow@pentagon.af.mil**) and HQ AFCA/EVPS (**afca.evps@scott.af.mil**) by electronic mail (E-mail), so their official listings can be updated with the new name, office symbol, phone number, and E-mail address. The MECO will:

9.1.1. Provide guidance and procedural policy to the ECOs on management of IT hardware assets.

9.1.3. Approve or reject transfer of IT assets between losing and gaining commands.

9.1.4. Send applicable ECO concerns about the inclusion and/or exclusion of IT hardware assets in AIM to SAF/XCI, 1401 Wilson Blvd, Ste 600, Arlington VA 22209-2315.

9.1.6. DELETED.

9.1.8. DELETED.

9.1.9. Coordinate on the establishment of a new DRA and the IT data system connectivity, as required.

9.1.9.1. Maintain a copy of the base ECO's appointment letter and AIM Access Request form. The MECO also sends the AIM Access Request to the program management office (PMO).

9.1.9.2. DELETED.

9.1.11. DELETED.

9.1.12. Disseminate information provided by HQ USAF, HQ AFCA, and PMO to applicable ECOs.

9.1.13. Establish accountability for IT assets acquired through joint services PMs, as required.

10. Equipment Control Officer (ECO).

10.1. The CSO appoints the primary and alternate ECOs according to paragraph **6.12.** See paragraph **15.** for contractors. Due in part to guidelines in AFPD 65-2, *Management Control Program*, the ECO cannot be the EC for the holding account. The unit commander must appoint a different individual as the EC to maintain a separation of duties.

10.1.1. In deployed locations, the forward commander appoints the most qualified individual available to perform the duties of ECO.

10.2. Determine the method used to account for IT according to paragraph **22.1.**

10.2.1. If the IT hardware should be accounted for in AIM, complete all necessary documentation and ensure the IT asset status in AIM is updated using the codes identified in **Attachment 5**. Review the IT asset status codes periodically to ensure the codes reflect the current status.

10.2.2. DELETED.

10.2.3. Assist the EC in determining the ownership of all FOB IT assets.

10.2.4. DELETED.

10.2.5. Direct ECs to conduct a complete annual inventory of all IT assets assigned to the EC's AIM account and an annual review of EC appointment letters to ensure the primary and alternate EC names are current and they have completed annual EC training. When possible, the EC appointment letter review should be held in conjunction with the annual inventory.

10.2.5.1. During the inventory, ensure all assets can be traced back to an AIM inventory listing. If IT hardware equipment is found in the work area that is not on the AIM inventory listing, refer to paragraph **22.1.** to determine if the IT equipment should be added to AIM to establish accountability.

10.2.5.2. In deployed locations, the forward commander determines the timeline for inventory based on rotation schedules.

10.2.5.3. ECOs have the authority to lock EC accounts until the annual inventory and EC training is completed.

10.2.6. DELETED.

10.2.7. Authorize the EC to retain serviceable excess IT asset items for maintenance redundancy or operational spares when allowed by the parent MAJCOM.

10.2.8. Retains unserviceable excess IT asset hardware for cannibalization as directed by the CSO.

10.2.9. Ensure correct MAJCOM code is entered into AIM for all IT assets in their DRA.

10.2.10. Provide the EC with AIM-generated standard product (bar code) labels.

10.2.11. Work with the EC to update the inventory as dictated by a ROS. Use a copy of the DD Form 200, **Financial Liability Investigation of Property Loss**, to adjust accountable records.

10.2.12. Complete out-processing for departing EC upon transfer of account and receipt of new appointment letters and signed joint loss-gain inventory.

10.2.13. Provide guidance and annual training for the EC. Upon request, the ECO provides their commanders with documentation verifying names of the ECs trained, material covered, and training dates.

10.2.14. Take guidance and direction from the MECO and CSO.

10.2.15. DELETED.

10.2.16. Code deployable IT assets in the AIM database.

10.2.17. Establishes accountability for IT hardware assets acquired through joint services, working with the parent MAJCOM.

10.2.18. Attempt to reutilize excess organizational IT assets that meet minimum architecture standards before offering equipment to organizations outside the DRA, when allowed by the parent MAJCOM.

10.2.19. DELETED.

10.2.20. DELETED.

10.2.21. After receipt of a transportation fund cite, direct the losing custodian to prepare the necessary shipping documents for items that are excess and required by other services.

10.2.22. DELETED.

10.2.22.1. DELETED.

10.2.23. DELETED.

10.2.24. DELETED.

10.2.25. Works with any tenant ECO to establish a host tenant agreement identifying any assistance required, such as AIM connectivity.

10.2.26. DELETED.

10.2.27. DELETED.

10.2.28. Coordinate on all host-tenant support agreements (HTSA) concerning IT asset management. IT accountability support can be specified in the HTSA or a Memorandum of Agreement (MOA).

10.2.29. DELETED.

11. Equipment Custodians (EC).

11.1. Accountable for all assigned IT hardware assets in their account and will:

11.1.1. Perform, at a minimum, an annual physical inventory of all items in the account. Also, conduct inventories when directed by the ECO. Upon completion of the inventory, the EC and the organizational commander or equivalent sign the inventory with the original copy retained by the EC and a copy for the ECO file.

11.1.2. Only the most current inventory is retained in the EC/ECO folder. Review past inventory records before disposing of old inventory data and ensure source documents are retained to support current inventory records, e.g., Reports of Survey, hand receipts, etc. Recommend using 6-part folders.

11.2. When practical (e.g., due to size limitations), ensure all accountable IT assets have AIM-generated standard product (bar code) labels affixed.

11.3. Obtain approval and coordinate all potential transfers of IT assets between EC accounts with the applicable ECO where practical.

11.4. Report all FOB IT assets to the applicable ECO and accept accountability or distribute equipment as directed by that ECO.

11.5. Sign for new equipment received through the ECO.

11.6. Take guidance from the ECO on all shipments, transfers, donations, or turns-ins of excess IT assets.

11.7. Provide appropriate documentation to the applicable ECO to clear the account of equipment that was shipped to another base/location, transferred to another account, donated to a school, or turned-in to the DRMO.

11.10. Conduct a joint physical inventory (outgoing EC with incoming EC) and reconcile any missing items, via ROS or hand receipt, before permanent change of station, permanent change of assignment, separation, or retirement (minimum of 30 days prior). Contact the individual to whom the equipment was issued, to verify the equipment's status.

11.11. DELETED.

11.12. Initiate the ROS process according to AFMAN 23-220, concerning any lost, damaged, or destroyed IT assets.

11.13. Notify the applicable ECO of excess IT assets.

11.14. Provide the applicable ECO a serialized numbered list of any deployed IT assets.

11.15. Receive and secure all IT assets, if not received by the ECO, until proper accountability is established.

11.16. Coordinate with the Information Systems Security Officer (ISSO) to ensure the ISSO sanitizes hard drives according to the procedures outlined in AFSSI 5020 (FOUO). Find additional information at **http://iase.disa.mil/policy.html**

12. DELETED.

13. DELETED.

14. Network and Computer Security. Refer to AFI 33-202, Volume 1.

14.1. DELETED.

14.2. DELETED.

14.3. DELETED.

15. Air Force Contractors. Organizational commanders grant contractors access to, or allow operation of, government-furnished or contractor-owned IT resources processing government information.

15.1. Contractors may function as equipment custodians (if so stipulated in the contract) for DOD-owned IT assets as the contract specifies.

15.2. According to the Federal Acquisition Regulation (FAR) 45.505, *Records and Reports of Government Property*, the contractor's property control records shall constitute the Government's official property records unless an exception has been authorized. The contractor shall establish and maintain adequate control records for all Government property, including property provided to and in the possession or control of a subcontractor.

15.3. Annually, the contractor's property control system shall provide to the contracting official, the total acquisition cost of Government property for which the contractor is accountable under each contract with each agency, including Government property at subcontractor plants and alternate locations. (Reference FAR Part 45.)

15.4. Establish the extent of contractor liability in the provisions of the applicable contract's government property clause. (See AFI 23-111.)

15.5. If a contractor is hired to accomplish ECO duties, the Air Force retains responsibility for obligating funds and receiving assets as they are inherently governmental functions. (See FAR 7.5, *Inherently Governmental Functions*)

15.6. The functions and responsibilities of the Accountable Officer are defined by DOD 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, January 2002. Accountable Officers exercise substantive discretionary authority in determining the Government's requirements and controlling Government assets. The responsibilities of the Accountable Officer and the position of the Accountable Officer are not contractible.

15.7. Contractors can perform functions in support of the Accountable Officer and functions where they are performing in accordance with criteria defined by the Government. For instance, contractors can process requisitions, maintain stock control records, perform storage and warehousing, and make local procurements of items specified as deliverables in the contract.

15.8. The responsibility for administrative fund control is inherently governmental. The contractor can process all required paperwork up to funds obligation, which must be done by the Government employee designated as responsible for funds control. The contractor can also process such documents as reports for survey and adjustments to stockage levels, but approval must rest with the Accountable Officer. In all cases, the administrative control of funds must be retained by the Government, since contractors or their employees cannot be held responsible for violations of the United States Code.

15.9. If the contractor's property control system does not automatically accomplish Chief Financial Officer asset reporting, then reporting will be accomplished manually according to Federal Financial Accounting Standards No. 6, dated 1996.

16. Acquisition of Information Technology (IT) Assets.

16.1. Procurement of desktops and laptops through AFWay is mandatory unless waived by the MAJCOM CIO/A6. Ordering information can be found at: **https://afway.af.mil**.

16.2. Requirements processing for IT assets not procured through AFWay are covered under AFI 33-103. Process all base user computer systems orders except those excluded by host tenant support agreements and Joint Service programs managed outside the Air Force through AFWay.

17. DELETED.

18. DELETED.

19. Use of Information Technology (IT) Systems.

19.1. Use IT assets for official or authorized purposes only. Commanders may authorize use of government resources for personal projects if they determine the use is in the best interest of the Air Force. Document the authorization in an organizational policy letter or by a letter to the individual concerned.

19.2. Do not input or store government information/data on privately owned IT assets without approval by the DAA according to AFI 33-202, Volume 1.

19.2.1. DELETED.

19.2.2. DELETED.

19.3. DELETED.

19.4. DELETED.

19.5. Alternate Work Locations. Unit commanders, in coordination with the local personnel office, may authorize personnel to work at an alternate work location (including the employee's home). Unit commanders may also authorize installation of a PC, applicable software, modems, facsimile machines, and data (telephone) lines to support access at the alternate duty location (see Federal Personnel Manual (FPM) System, FPM Letter 368-1, 26 March 1991, "Federal Flexible Workplace Project;" and Public Law (PL) 104-52, *Telephone Installation and Charges*, STAT 468, Section 620 [31 U.S.C. 1348]). Commanders must consider the cost of providing necessary communications and IT assets services before allowing personnel to work from an alternate duty location.

19.5.1.6. Coordinate and document all equipment relocations with the EC before relocating assets.

19.5.1.7. DELETED.

19.5.3. Prepare a letter for the individual to sign acknowledging their understanding of the basic network security policy. It is also recommended that users complete the Information Assurance Awareness CBT for knowledge and understanding of responsibilities regarding Information Assurance and protection.

19.5.3.1. As a minimum, the letter should stipulate that personal IT equipment cannot be used to store, receive, or process classified information and that all chat/instant messenger programs must be disabled on privately owned information systems.

19.5.4. See AFI 33-202, Volume 1, for additional guidelines on telecommuting.

19.5.5. The authorizing unit will keep those letters on file for the duration of the telecommuters' assignment to that unit. After that, file according to the appropriate rule in AFRIMS RDS, Table T33-07 located at **https://afrims.amc.af.mil/rds_series.cfm**.

20. (DOES NOT APPLY TO ANG) General Officers (GO) and Senior Executive Service (SES) Notebook Computers and Personal Digital Assistants (PDA).

20.1. Active Duty GO and SES personnel, including brigadier general selects, are required to maintain E-mail contact with the Chief of Staff of the Air Force. The GO's or SES' current unit of assignment will purchase a GO and SES notebook computer/PDA through the local communications unit and follow the standard requirement process. If desired by the GO or SES, the notebook computer/PDA may accompany the GO or SES from assignment to assignment. If GOs or SES' decide to take their notebook computer/PDA, they will work with the losing and gaining communications unit to ensure proper inventory accountability. The local EC retains accountability for the notebook computer/PDA until transferred to the new location. (See AFI 33-202, Volume 1.)

20.1.1. DELETED.

20.1.2. When a GO or SES retires or leaves Air Force service; he or she must turn in the notebook computer/PDA to the supporting ECO.

Section C--Inventory, Accountability, Transfer, and Reporting of Information Technology (IT) Systems

***NOTE*:** Consult AFI 33-115, Volume 1 for additional guidance in determining the types and quantities of equipment needed to support the network.

22. Inventory Management and Accountability of IT Hardware Assets.

22.1. Guidance for determining the accountability of IT assets is governed by multiple and complex congressional, federal, DOD, and Air Force policies. In order to simplify the determination of Air Force accountable IT assets, a comprehensive and current list of accountable and non-accountable assets is posted and maintained on the Air Force Portal (**https://www.my.af.mil**) under the Enterprise IT Initiatives section.

22.1.1. Management and oversight of the official Air Force accountability list is the responsibility of the CSMWG.

22.1.2. DELETED.

22.2. DELETED.

22.3. DELETED.

22.4. IT resources are shipped to the ECO and marked for the appropriate EC.

22.5. Software purchased with original equipment manufacturer IT is considered an integral part of the system. Therefore, the software must be maintained with the system. If the system is transferred, software and system documentation must accompany the system. Transfer all documentation with the system.

22.6. Software license management is explained in AFI 33-114.

22.7. IT assets that are components of weapons systems or other major systems and are already tracked in AFEMS or another property management system will not be tracked in AIM.

22.8. Equipment that is deployed and remains in possession/use of home station personnel who are deployed should be tracked and managed within the home station inventory. Equipment that is transferred to other units or left forward must be properly transferred from the home station (losing unit) account to an appropriate gaining unit to maintain full accountability.

23. DELETED.

24. DELETED.

25. DELETED.

26. Transferring Non-excess Information Technology (IT) Assets to another Department of Defense Component, Federal Agency, State, or Local Government. The transfer of non-excess IT assets occurs when a function, and the IT assets acquired to support that function, is transferred to another DOD component or Federal agency.

26.1. The losing EC provides the losing ECO with a letter of transfer, signed by the losing commander documenting the transfer of the function and equipment.

26.2. Ensure a DD Form 1149, **Requisition and Invoice/Shipping Document**, is signed and dated by a designated official from the shipping activity (Traffic Management Office or commercial carrier) and the EC. For local transfers where no shipping activity is involved, the gaining and losing EC signs the DD Form 1149.

26.3. The ECO for the losing activity should account for the transferred IT. The ECO should also identify excess IT created as a result of the transfer of a function.

26.3.1. The losing ECO and the gaining ECO or other accountable officer will:

26.3.1.1. Review contracts to terminate maintenance for excess equipment.

26.3.1.2. Assist contracting officials in the transfer of responsibilities to the gaining activity.

26.4. The losing ECO will:

26.4.1. Update the asset status field in AIM using the codes in **Attachment 5**.

26.4.2. Provide information for accountable records to the gaining activity if the gaining activity is not using the same database as the losing activity.

26.4.3. Review all contract obligations with the gaining and losing activity. Pay close attention to any contract termination clauses (applies when extra maintenance has been paid for by the losing organization). Use currently established AIM guidance for the removal of items from an account.

26.4.4. Review IT assets release dates. Give adequate notice to the vendor to preclude payment of extra costs.

26.4.5. Coordinate IT assets release dates with other base functions, if necessary.

26.4.6. Coordinate with ISSO for hard drive sanitation according to the procedures outlined in AFSSI 5020 (FOUO). Find additional information at **http://iase.disa.mil/policy.html**.

26.4.7. Provide the IT system database records or custodian report for the EC to attach to the equipment being transferred as appropriate.

26.4.8. Properly inventory, package, warehouse, and secure equipment when storing IT assets before transfer.

26.4.9. Ensure the IT system database inventory records reflect this transfer of equipment accountability to the receiving organization.

26.4.10. Ensure the AFEMS Help Desk is notified to delete or archive the IT records of the equipment being transferred to a Department of Defense Component, Federal Agency, State, or Local Government.

Section D--Information Technology (IT) Systems Maintenance **(Not Applicable to Non-Air Force Managed Joint Service Systems)**

27. Support Plan. The CSO develops a Logistics Support Plan for IT assets according to AFI 21-116 to ensure logistics support throughout the expected lifecycle. A support plan includes planning and developing a spare and repair parts support plan, determining initial requirements, acquisition planning, distribution, and replenishment of inventory spares.

27.1. Although there is no one size fits all method to determine the quantity of spare equipment or repair parts to keep on hand, consider technical data such as mean time between failure rates, reliability data obtained from the manufacturer, and order and ship time from the source of supply when analyzing supply support. Personnel should also consider mission impact factors such as single point of failure and/or mission critical items. Ultimately it is the commander's or maintenance superintendent's decision based on past experience for low density/commercial off-the-shelf systems that determine the number of on-hand spares to ensure mission accomplishment.

27.1.1. Regardless of the method used to determine the quantity of spare equipment or repair parts to keep on hand, the rationale/methodology used to determine the quantity must be documented in the Logistics Support Plan.

NOTE: Consult AFI 33-115, Volume 1, for additional guidance in determining types and quantities of equipment needed.

27.2. DELETED.

27.2.1. DELETED.

27.2.2. DELETED.

27.2.3. DELETED.

27.3. DELETED.

27.4. DELETED.

27.5. DELETED.

27.5.1. DELETED.

27.5.2. DELETED.

27.5.3. DELETED.

27.6. Maintenance Management. Maintenance management requirements are necessary to avoid risks to personnel, prevent damage to IT hardware equipment, and ensure IT equipment availability to meet mission requirements (Refer to AFI 21-116, AFI 33-115, Volume 1, and AFI 33-series guidance).

27.7. Personnel performing maintenance tasks on IT hardware follow the maintenance management requirements for mission critical and non-mission critical items according to AFI 21-116.

27.8. The headquarters or field-level unit determines if the IT hardware is considered mission critical or non-mission critical for maintenance management purposes.

27.9. Cannibalization may be used to satisfy an existing requirement and to meet priority mission requirements.

27.10. Technical Order 00-20-2, *Maintenance Data Documentation*, outlines the cannibalization process and documentation requirements.

27.11. When cannibalization is the only option available, identify the end item to be cannibalized, and request approval from the chief of maintenance/chief of mission systems flight, computer systems officer or designated representative according to AFI 21-116.

27.12. The CSO or designated representative can approve cannibalization of non-mission critical IT equipment, however; the CSO ensures procedures are developed to ensure non-mission critical cannibalized IT assets are restored to full operational capability if economically feasible.

27.13. Maintenance actions to obtain assemblies, sub-assemblies, or parts are considered transfers and are not treated as cannibalization actions. The CSO may retain assemblies, sub-assemblies, or parts from spare IT assets for maintenance redundancy and operational spares when the communications unit has a maintenance or operational support mission.

27.14. The CSO may also approve the use of unserviceable IT hardware assets as a source for spare parts to maintain other IT equipment. This authority should only be used when allowed by the parent MAJCOM and a cost analysis clearly determines it is economically feasible to use excess assets instead of procuring new items.

27.15. Assemblies, sub-assemblies, and parts obtained for maintenance redundancy or operational spares using the methods described in paragraphs 23.4 and 23.5 are accounted for in the AIM. Ensure the IT

asset status in the AIM is updated to identify these items as operational spares. Asset status codes are listed in **Attachment 5**.

28. DELETED.

29. Information Technology (IT) Systems Maintenance Reporting. Users with maintenance contracts document all IT asset maintenance on AF Form 597, or vendor maintenance forms as specified in the appropriate contract. If AF Form 597 is used, provide a copy to the vendor. Each MAJCOM CIO/A6 will specify procedures for logging, documenting, collecting, processing, and filing copies of maintenance records in accordance with the AFI 37-100 series publications (will convert to AFI 33-300 series publications).

30. DELETED.

31. DELETED.

32. Computation of Payments. Contracts applying to managed IT assets.

32.1. Effective Start Date for Rental or Lease. The effective date for rented/leased IT assets is usually the first day of the successful acceptance test. A government-caused acceptance test delay may require payment for the delayed period. Consult the individual contract for specific guidance.

32.2. Computing Charges. ECOs compute charges for rented/leased IT assets, using the reverse side of AF Form 597 or locally produced vendor form.

32.3. Validating Services. For Air Force-managed systems, the verifying activity refers to the equipment utilization reports and the input to the reports (IT assets/equipment orders, AF Form 597, and other appropriate records), to validate the services. Submit claims for credit within 60 days (or as stated in the contract). The IT assets contract manager designates the verifying activity for non-Air Force managed systems (e.g., joint service systems).

Section E--Disposition of Excess Information Technology (IT) Resources

33. Excess. An item is considered excess when it is no longer required due to mission change, equipment upgrades, technology changes, obsolescence, etc. The item is also considered excess when the total quantity on hand exceeds the required quantity, as identified in the technical solution/requirements document, plus the number of authorized spares as identified in the Logistics Support Plan. According to AFI 23-111, accountable individuals are responsible for properly identifying, reporting, and determining correct disposition of unserviceable, reparable, or excess property.

33.1. Base or MAJCOM CSOs may develop their own policies for the retention of excess IT assets, to include potential reutilization (see AFSSI 5020 [FOUO]). However, the rationale for the retention policy must be documented; preferably in the Logistics Support Plan.

33.2. The EC notifies the ECO when IT assets become excess. If possible, ECs should provide notification 30 days before the equipment goes off line to allow completion of the screening cycle while the equipment is still in use, eliminating the need to store excess assets. Until receipt of final disposition instructions, the EC stores the equipment to prevent damage, deterioration, or unauthorized cannibalization.

33.3. Excess Air Force assets can be located using DRMS.

33.4. Disposition of excess classified media. The ISSO or designated representative signs and affixes the appropriate disposition certification label and marks classified media as required according to the guid-

ance in AFI 31-401 . Also, all personnel handling classified materials bear a responsibility to ensure their media is appropriately marked. ***NOTE***: For your use, DLA has developed a label, based on the information required in ASD Memorandum, June 4, 2001. This is an optional form. Please note that it also contains a block to check if you are turning in housings where the hard drive has been removed. This form can be printed on sticky labels, i.e., Avery 5164 or Pres-a-ply 30604 (reference AFSSI 5020 [FOUO] and AFI 31-401).

33.5. DELETED.

33.6. DELETED.

33.7. DELETED.

33.8. DELETED.

33.9. DELETED.

33.10. DELETED.

34. Obtaining Excess Resources. If the parent MAJCOM allows the use of excess IT to satisfy new requirements, the ECOs review excess redistribution programs and reports to determine if suitable excess resources are available.

34.1. The ECO may direct reutilization of IT assets to replace equipment that does not meet minimum standards when allowed by the parent MAJCOM.

34.2. To acquire equipment from the DRMO, the EC submits documentation (DD Form 1348A-1, **Issue Release/Receipt Document**) for coordination to the ECO. Assets can either be viewed at the DRMO location or researched at **http://www.drms.dla.mil/rtda/**.

34.3. ECOs establish accountability in the AIM for IT hardware equipment acquired through any source that meets the criteria for accountability in paragraph **22.1.**

35. Transferring Excess Information Technology (IT) Systems Assets to the Defense Reutilization Marketing Office (DRMO).

35.1. DRMO is the primary source for disposal of all military property and equipment. All Air Force IT (accountable or non-accountable) when practical, should be disposed of through the DRMO.

35.2. DRMO guidelines for excess and the disposal of IT assets can be found at **http://www.drms.dla.mil/rtd03/dodit.htm**.

35.3. All hard drives for IT assets being disposed of or transferred to DRMO within or outside of the DOD will be sanitized (i.e. overwriting, degaussing, or destroying) according to AFSSI 5020 (FOUO).

35.4. ECO's must establish a MOA with their servicing DRMO in order to transfer IT equipment directly to local schools under the Computers for Learning Program. Donations of IT equipment to schools can only take place AFTER completion of the mandatory DOD reutilization screening and then the IT equipment may be donated only to registered and qualified institutions identified by the DRMS.

35.4.1. The Air Force cannot donate IT assets directly to a school without the approval or knowledge of the DRMO.

35.5. The trade-in of Air Force IT assets is an allowable excess transaction under the provisions outlined in AFPD 23-5, *Reusing and Disposing Of Materiel*, as long as the transaction results in measurable sav-

ings to the Air Force. Additional guidance regarding equipment exchanges related to credit or warranty action is addressed in AFMAN 23-110, Volume 2, Part 13, Chapter 8.

35.5.1. Adherence to remanence security requirements is vital to all transactions relating to excess IT, whether they are credit or warranty exchanges or direct disposals to the DRMO.

36. DELETED.

37. DELETED.

38. Information Collections, Records, and Forms and Information Management Tools (IMT).

38.2. Records. Records generated are maintained according to AFRIMS RDS located at **https://afrims.amc.af.mil/rds_series.cfm**.

38.2.1. AIM: use Table 33-7, Rule 8 disposition schedules to delete/dispose of information.

38.2.2. Completed Checklist (AF Form 2519): use Table 37-15, Rule 31.

38.2.3. IT Inventory: use Table 33-7, Rule 12; and cannibalizations (Spare parts) records: use Table 23-3, Rule 6.

38.3. Forms or IMTs (Adopted and Prescribed):

38.3.1. Adopted Forms or IMTs. DD 200, **Financial Liability Investigation of Property Loss**; and DD Form 1149, **Requisition and Invoice/Shipping Document**; DD Form 1348A-1, **Issue Release/Receipt Document**; AF IMT 847, **Recommendation for Change of Publications**; AF IMT 2519, **All Purpose Checklist**;

38.3.2. Prescribed Forms or IMTs. AF IMT 597, **ADPE Maintenance Record**.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

PL 104-52, *Telephone Installation and Charges*, page 109 STAT 468, Section 620 (31 U.S.C. 1348)

E.O. 12999, *Education Technology: Ensuring Opportunity for All Children in the Next Century*

ASD Memorandum, Disposition of Unclassified DOD Computer Hard Drives, June 4, 2001: **http://www.drms.dla.mil/turn-in/#harddrive**

DODD 8000.1, *Management of DOD Information Resources and Information Technology*, February 27, 2002, with Change 1, March 20, 2002

DODD 8100.1, *Global Information Grid (GIG) Overarching Policy*, September 19, 2002

DODI 4100.33, *Commercial Activities Program Procedures*, September 9, 1985, with Change 3, October 6, 1995

DODI 5000.64, *Defense Property Accountability*, August 13, 2002

DODI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

DOD 4140.1-R, *DOD Supply Chain Materiel Management Regulation*, May 23, 2003

DOD 5500.7-R, *Joint Ethics Regulation (JER)*, August 1993, with Change 4, August 6, 1998

DOD 7000.14-R, Volume 12, *Special Accounts, Funds and Programs*, January 2002

AFPD 10-6, *Mission Needs and Operational Requirements*

AFPD 23-5, *Reusing and Disposing Of Materiel*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems* (will become Information Resources Management)

AFPD 33-2, *Information Protection* (will become *Information Assurance*)

AFPD 65-2, *Management Control Program*

AFI 10-1401, *Modernization Planning Documentatio*n

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*

AFI 21-116, *Maintenance Management of Communications-Electronics*

AFI 23-111, *Management of Government Property in Possession of the Air Force*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-104*, Base-Level Planning and Implementation*

AFI 33-114, *Software Management*

AFI 33-115, Volume 1, *Network Operations (NETOPS)*

AFI 33-202, Volume 1, *Network and Computer Security*

AFI 63-124, *Performance-Based Service Contracts (PBSC)*

AFI 65-501, *Economic Analysis*

AFMAN 23-110, *USAF Supply Manual*

AFMAN 23-220, *Reports of Survey for Air Force Property*

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

AFSSI 5020, (FOUO) *Remanence Security*

AFWay Users Guide

FAR 7.5, *Inherently Governmental Functions*

FAR 45.505, *Records and Reports of Government Property*

DFAR Supplement, Part 217.70, *Exchange of Personal Property*

Uniform Code of Military Justice

FPM Letter 368-1, 26 March 1991, Federal Flexible Workplace Project

Technical Order 00-20-2, *Maintenance Data Documentation*

AFRIMS RDS (**https://afrims.amc.af.mil/rds_series.cfm**)

Federal Financial Accounting Standards No.6, dated 1996

Abbreviations and Acronyms

AF	Air Force (used on forms only)
AFEMS	Air Force Equipment Management System
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFRIMS	Air Force Records Information Management System
AFSSI	Air Force Systems Security Instruction
AFWay	Air Force Way
AIM	Asset Inventory Management
AIS	Automated Information System
ANG	Air National Guard
ASD	Assistant Secretary of Defense
C4	Command, Control, Communications, and Computer
C-E	Communications- Electronics
CBT	Computer Based Training
CPU	Central Processing Unit

CSA Client Support Administrator
CSM Computer Systems Management
CSMWG Computer Systems Management Working Group
CSO Communications and Information Systems Officer
DAA Designated Approving Authority
DD Department of Defense (used on forms only)
DFAR Defense Federal Acquisition Regulation
DFAS Defense Finance and Accounting Service
DLA Defense Logistics Agency
DOD Department of Defense
DRA Defense Reporting Activity
DRMO Defense Reutilization and Marketing Office
DRU Direct Reporting Unit
E.O. Executive Order
E-mail Electronic Mail
EA Economic Analysis
EC Equipment Custodian
ECO Equipment Control Officer
FAR Federal Acquisition Regulation
FOA Field Operating Agency
FOB Found-On-Base
GO General Officer
HTSA Host Tenant Support Agreement
HQ AETC Headquarters Air Education and Training Command
HQ AFCA Headquarters Air Force Communications Agency
HQ OSSG Headquarters Operations and Sustainment Systems Group
HQ SSG Headquarters Standard Systems Group
IA Information Assurance
ISSO Information Systems Security Officer
IT Information Technology
MAJCOM Major Command
MECO Major Command Equipment Control Officer

MOA Memorandum of Agreement

MSG Material Systems Group

NCO Noncommissioned Officer

OPR Office of Primary Responsibility

PA Program Agreement

PBSC Performance Based Service Contracts

PC Personal Computer

PDA Personal Digital Assistant

PL Public Law

PM Program Manager

PMO Program Management Office

RDS Records Disposition Schedule

ROS Report of Survey

SAF Secretary of the Air Force

SES Senior Executive Service

USAF United States Air Force

Terms

Accountable Officer An individual appointed by proper authority who maintains items and/or financial records in connection with government property, irrespective of whether the property is in his or her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use or care and safekeeping. In all cases, the accountable officer is responsible for establishing and maintaining financial property control records, controlling the processing of supporting documentation, and maintaining supporting document files. The primary accountable officers under the Air Force ROS System include: chief of supply, medical supply officer, munitions officer, fuels officer, communications and information systems officer, civil engineer, etc.

Cannibalization Authorized removal of a specific assembly, subassembly or part from one system for installation on another end item to satisfy an existing supply requisition and to meet priority mission requirements with an obligation to replace the removed item. Canning is the act of removing serviceable parts from one IT system for installation in another IT system when removal of parts will cause the first system to not perform as designed.

C-E Maintenance Any action taken to restore C-E equipment to operational status, to perform preventive maintenance inspections on C-E equipment, or to install or remove C-E equipment.

C-E Equipment All communications systems and equipment including but not limited to ground-based radio and wireless systems including infrared; radar, meteorological and navigational radiation aids used for aircraft control and landing; radiating aids for fire control; imagery, video processing equipment and intrusion detection systems, satellite, microwave and telemetry equipment; mission critical computer hardware, telecommunications switching equipment, cable and antenna systems; cryptographic equip-

ment and communications consoles; and electronic counter-measures and related radiation, re-radiation, and electronic devices.

Central Processing Unit (CPU) The portion of a computer that executes programmed instructions, performs arithmetic and logic functions, and controls input and output functions. One CPU may have more than one processor housed in the unit.

Client Support Administrator (CSA) The primary point of contact for computer related problems. The person appointed and certified under AFI 33-115, Volume 1 to support information systems/technology related tasks. Formerly Workgroup Manager (WM).

Command, Control, Communications, and Computer (C4) System An integrated system of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control through all phases of the operational continuum. This system includes visual information support systems. Within the Air Force referred to as communications and information systems.

Communications and Information Systems Officer (CSO) The term CSO identifies the supporting systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities. At MAJCOM and other activities responsible for large quantities of communications and information systems, it is the person designated by the commander as responsible for overall management of systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol SC that is expanded to three and four digits to identify specific functional areas. CSOs are accountable officers for all automated data processing equipment in their inventory.

Computer System A functional unit, consisting of one or more computers and associated software, that (1) uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program; (2) executes user-written or user-designated programs; and (3) performs user-designated data manipulation, including arithmetic and logic operations. ***NOTE:*** A computer system is a stand-alone system or may consist of several interconnected systems. Personal computers, microcomputers, minicomputers, multi-user systems, all standard multi-user small computer requirements contract systems, text processors, word processors, intelligent typewriters, and workstations are examples of computer systems.

Department of Defense (DOD) Redistribution Program Worldwide program, initiated by DOD for reporting, screening, redistributing, and disposing of automation resources that have become excess under an original application.

Designated Approving Authority (DAA) Official with the authority to formally assume responsibility for operating an information system or network within a specified environment. (AFI 33-202, Volume 1)

Documentation: The formal standardized recording of detailed objectives, policies, and procedures governing conception, authorization, design, testing, implementation, operation, maintenance, modification, and disposition of data administration techniques and applications.

Economic Analysis (EA) An EA helps us make rational choices among competing alternatives. A good EA systematically examines and tells us about costs, benefits, and risks of various alternatives.

Equipment Control Officer (ECO) An individual appointed by the applicable CSO to manage and control IT assets resources for a base. (***NOTE:*** A tenant unit may have its own ECO. This should be coordinated among the main base Communications unit, the tenant unit, and the MAJCOM of the tenant unit.)

Equipment Custodian (EC) An individual who acts as a subordinate to the applicable ECO and performs inventory, utilization, and maintenance recording and reporting and other custodial duties as the ECO requires.

Hardware (1) The generic term dealing with physical items as distinguished from its capability or function such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, and parts. The term is often used in regard to the stage of development, as in the passage of a device or component from the design stage into the hardware stage as the finished object. (2) In data automation, the physical equipment or devices forming an IT system and peripheral components. See also **software**.

Information Systems Security Officer (ISSO) Official who manages the computer security program for an information system assigned to him or her by the Information Systems Security Manager; including monitoring information system activities, and ensuring that the information system is operated, maintained, and disposed of according to security policies and practices. (***NOTE:*** See DODI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003.) An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DOD information system or organization. While the term IAO is favored within the DOD, it may be used interchangeably with other IA titles (e.g., Information Systems Security Officer, Information Systems Security Custodian, Network Security Officer, or Terminal Area Security Officer). (AFI33-202, Volume 1).

Information Technology (IT) Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DOD component. For the purposes of the preceding sentence, equipment is used by a DOD component if the equipment is used directly or is used by a contractor under a contract with the DOD component that (1) requires the use of such equipment; or (2), requires the use to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term Information Technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services) and related resources. Notwithstanding the above, the term information technology does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (See DOD Directive 8000.1, *Management of DOD Information Resources and Information Technology*, February 27, 2002, with Change 1, March 20, 2002.) ***NOTE***: The focus of this instruction is IT hardware management. AFI 33-114 is the governing Air Force instruction for software.

Joint Service System A standard system implemented at one or more services sites (U.S. Army, U.S. Navy, U.S. Air Force, and U.S. Marine Corps). Systems acquisition, development, maintenance, and life-cycle support are assigned to a program manager assigned to one of the services.

Life-Cycle Management (1) The management of a system or item, starting with the planning process and continuing through successive management processes and associated life-cycle management phases and associated milestones, until a system is terminated. (2) A management process, applied throughout the life of an AIS that bases all programmatic decisions on the anticipated mission-related and economic benefits derived over the life of the AIS.

Maintenance (1) All action taken to retain materiel in or to restore it to a specified condition. It includes: inspection, testing, servicing, classification as to serviceability, repair, rebuilding, and reclamation. (2) All supply and repair action taken to keep a force in condition to carry out its mission. (3) The routine recurring work required to keep a facility (plant, building, structure, ground facility, utility system, or

other real property) in such condition that it is continuously utilized, at its original or designed capacity and efficiency, for its intended purpose. (4) The function of keeping C4 items of equipment in, or restoring them to, serviceable condition. Maintenance is not intended to increase the value, capabilities, or expected life of a system. Equipment maintenance includes servicing, repair, modification, modernization, overhaul, inspection, condition determination, corrosion control, and initial provisioning of support items. Maintenance includes both preventive and corrective actions. Software maintenance includes anticipating, detecting, and eliminating errors.

Major Command Equipment Control Officer (MECO) The individual appointed by the CSO that oversees the management and control IT assets for the MAJCOM, FOA, and DRU.

Peripheral Any equipment that provides the IT system with additional capabilities distinct from the central processing unit (e.g., a printer, mouse, disk drive, digitizer, etc.).

Pilferable Items having a ready resale value, civilian utility or application, and therefore are especially subject to theft. Consideration must be given to the cost to provide controlled storage and handling compared to the potential losses when selecting items to be treated as pilferable items. Generally an item should not be coded for worldwide treatment as pilferable, unless the unit cost exceeds $100 and repetitive losses indicate the item is subject to theft; however, the unit cost criteria may be waived when management determines that losses on an item warrant the cost of additional controls.

Resources Any IT system, component hardware and software, contractual services, personnel, supplies, and funds.

Shareware Privately or commercially developed software that is normally distributed free of charge but a fee is generally expected for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent.

Software (1) A set of IT assets programs, procedures, and associated documentation concerned with the operation of an IT system (i.e., compilers, library routines, manuals, circuit diagrams). (2) The programs, procedures, rules, and any associated documentation pertaining to the operation of data processing systems.

System A set of IT components and their external peripherals and software interconnected with another set. Typical systems include notebook computers, desktop PCs, networked and distributed systems (e.g., servers, workstations, data management processors, etc.), mainframe and midsize computers and associated peripherals.

Systems Administrator The organization focal point for multi-user systems.

Attachment 2

DELETED

Attachment 3

INFORMATION TECHNOLOGY (IT) SYSTEMS CHECKLIST

Table A3.1. Questions for Information Technology (IT) Systems Checklist.

#	ITEM	REFERENCE	Y	N	NA
	Equipment Control Officer (ECO)				
1	Is a copy of AFI 33-112 available?				
2	Has the CSO appointed a primary and alternate ECO in writing? Does the selected individual meet the criteria as noted in AFI 33-112?	AFI 33-112, paragraphs **6.12.** and **10.1.**			
3	Does the ECO receive all computer systems, ensuring accountability and completion of all necessary documentation?	AFI 33-112, paragraph **10.2.1.** and **22.1.**			
4	Does the ECO account for IT, according to AFI 33-112, utilizing AIM?	AFI 33-112, paragraph **10.2.**			
5	Is the ECO accountable for equipment listed in their assigned AIM account?	AFI 33-112, paragraph **10.2.2.**			
6	Does the ECO assist the EC in determining ownership of all FOB IT assets and takes appropriate action to ensure accountability?	AFI 33-112, paragraph **10.2.3.**			
7	Does the ECO direct all ECs to conduct an annual physical inventory of assigned computer systems?	AFI 33-112, paragraph **10.2.5.**			
8	Does the ECO ensure completion of the annual physical inventory and that EC appointments are renewed annually?	AFI 33-112, paragraphs **10.2.5.**			
9	Does the ECO prepare AIM bar code labels and provide them to the EC as needed?	AFI 33-112, paragraph **10.2.10.**			
10	Does the ECO work with the EC to update the inventory as dictated by a ROS?	AFI 33-112, paragraph **10.2.29.**			
11	Does the ECO complete out-processing for departing ECs upon transfer of account and receipt of new appointment letters?	AFI 33-112, paragraph **10.2.12.**			
12	Does the ECO provide guidance and training for the ECs?	AFI 33-112, paragraph **10.2.13.**			
13	Does the ECO receive guidance and direction from the MECO?	AFI 33-112, paragraph **10.2.14.**			

#	ITEM	REFERENCE	Y	N	NA
14	Does the ECO correctly code deployed computer systems in AIM as directed by HQ USAF or MAJCOM and authorized by the applicable CSO?	AFI 33-112, paragraph **10.2.16.**			
15	Does the ECO attempt to reutilize excess organizational IT assets that meet minimum architecture standards before offering equipment to organizations outside the DRA, when allowed by the parent MAJCOM?	AFI 33-112, paragraph **10.2.18.**			
16	Does the ECO works with any tenant ECO to establish a host tenant agreement identifying any assistance required, such as AIM connectivity?	AFI 33-112, paragraph **10.2.25.**			
17	Does the ECO coordinate on all host tenant agreements?	AFI 33-112, paragraph **10.2.28.**			
	Equipment Custodian (EC)				
18	Are ECs and alternates appointed in writing by the organizational commander?	AFI 33-112, paragraph **7.5.**			
19	Are ECs responsible for all assigned IT hardware assets?	AFI 33-112, paragraph **11.1.**			
20	Do the ECs perform an annual physical inventory of all items in the account? Upon completion, does the EC and the organizational commander or equivalent sign the inventory with the original copy retained by the EC and a copy for the ECO file?	AFI 33-112, paragraph **11.1.1.**			
21	Does the EC ensure all accountable IT hardware equipment has an AIM bar code label attached when practical?	AFI 33-112, paragraph **11.2.**			
22	Does the EC obtain approval and coordinate all potential transfers of computer systems between accounts with the applicable ECO? ***NOTE***: ECs have no authority to transfer computer systems outside their account.	AFI 33-112, paragraph **11.3.**			
23	Does the EC sign for new equipment received through the ECO?	AFI 33-112, paragraph **11.5.**			
24	Does the EC provide appropriate documentation to the applicable ECO to clear the account of equipment that was shipped to another base/location, transferred to another account, donated to a school, or turned-in to DRMO?	AFI 33-112, paragraph **11.7.**			
25	Has a joint physical inventory been accomplished prior to equipment account transfer?	AFI 33-112, paragraph **11.10.**			

#	ITEM	REFERENCE	Y	N	NA
26	Does the EC out-process through the applicable ECO?	AFI 33-112, paragraph **11.9.**			
27	Does the EC initiate the ROS process according to AFMAN 23-220, concerning any lost, damaged, or destroyed IT assets?	AFI 33-112, paragraph **11.12.**			
28	Does the EC provide the applicable ECO a serialized numbered list of deployed IT assets?	AFI 33-112, paragraph **11.14.**			
29	Does the EC receive and secure all IT assets, if not received by the ECO, until proper accountability is established?	AFI 33-112, paragraph **11.15.**			

Attachment 5

EQUIPMENT STATUS REPORTING

A5.1. The status codes in **Table A5.1.** describe the operational status of a component or DRA. Valid values are:

Table A5.1. IT asset status codes for equipment status reporting.

Status Code	Status Description
01	Programmed, planned, or unapproved order.
02	Approved acquisition, or on order.
03	Received on-site, but not installed.
04	Undergoing acceptance testing, during installation.
11	Installed, accepted, and in use.
12	Available excess.
41	Discontinued use.
52	Transferred in from another DRA.
	Operational spare—backup/safety item available to prevent critical failures to network/system. ***NOTE:*** At the time of publication, the AIM system could not be updated to reflect this status code due to funding limitations. Until the system is updated, users may use the Remarks field in AIM to annotate an asset as an operational spare.